Blog Archive - SpamTitan Email Security

By G Hunt

Archived: 2026-04-05 19:50:54 UTC

DKIM Replay Phishing Attempt Spoofs Google and Passes Validation Checks

by | April 30, 2025 | Phishing & Email Spam

Hackers have exploited a ‘vulnerability’ to conduct a phishing campaign that made it appear that the phishing email had been sent by Google from the no-reply[@]accounts.google.com address. The email was signed by Google and passed the DomainKeys Identified Mail (DKIM) authentication check, suggesting the email had been sent from a genuine Google account and was authentic, although the email had been sent from a different, non-Google address.

The campaign was identified by developer Nick Johnson, who received an email seemingly sent from no-reply[@]accounts.google.com with the subject Security Alert. The email claimed that Google LLC had been subpoenaed to obtain a copy of the contents of his Google account and that a support case had been opened and transferred to Legal Investigations Support. A support reference number was included along with a link to a Google Sites website, encouraging him to click the link to examine the case materials and “submit a protest,” if necessary, via the option on the support website.

The lure used in this phishing attempt is similar to many other phishing campaigns that threaten legal action or warn about police investigations, although what makes the attempt stand out is how the phisher managed to make the email appear to have been sent by Google and pass the DKIM authentication check, resulting in the email being delivered to his inbox.

While the subject matter was potentially serious, and the email had seemingly been sent by Google, there was a red flag that suggested a phishing attempt. As was noticed by Johnson, the link in the email did direct him to an official Google site, but it was sites.google.com, a free web-building platform provided by Google for users to create and host free web pages for personal purposes. No official email from Google would direct a user to that platform, and certainly not any message about a subpoena requiring the disclosure of the contents of their Google email account. The link directed Johnson to a fake support portal – a carbon copy of the official support portal, which had been scraped from the official site. The aim of the phish appears to have been to trick Johnson into logging in and disclosing his login credentials, allowing his Google account to be hijacked.

An analysis of the phishing attempt revealed Google was tricked into signing the email, thus allowing the message to bypass spam filtering service since the email successfully passed the DKIM and DMARC authentication checks. Closer inspection of the message header revealed the mailed-by address was different from the from address, and had been sent in what is known as a DKIM replay attack.

The message was actually sent to a me@ address at a domain that appeared to be managed by Google. According to Johnson, the attackers registered a domain and created a Google account for the me[@]domain.com, then

created a Google OAuth app and used the entire phishing message for its name, which was then added to the name field. They granted themselves access to the email address in Google Workspace, then Google sent an alert to the me[@]domain.com account. The email was then forwarded to Johnson, and since the email had been generated by Google, it was able to pass the DKIM check as the parts of the message that DKIM checks had not been altered.

The vulnerability that was exploited was the fact that DKIM checks the message and the headers, not the envelope, which meant the email passed the validation checks because it had a valid signature. Since the exact email was extracted and saved without making any modifications to what was signed by DKIM, the validation checks were passed. Further, since the email was sent to a me@ email address, it shows that the message was delivered to the victim's email address. Google explained in response to a query that it is aware of the phishing attempt and has rolled out protections to prevent further abuse.

The phishing attempt demonstrates the importance of stopping and thinking before clicking on any link in an email, no matter how serious the potential threat. The phishing attempt could have easily led to a compromised Google account had he not stopped to think about the request. Others may not have been as fortunate. While this was the first time that Google is known to have been affected by a DKIM replay attack, it is a known phishing technique and one that can be highly effective.

Security awareness training should make it clear that all emails can potentially contain a threat, even if the sender appears to be legitimate. Phishing lures related to legal threats, police investigations, and subpoenas should be included in the training as these are likely to create the fear that leads to a rapid click, and employees should be told to inspect the message headers to see the sender's address and told to report any potential threat or suspicious email to their security team. They should also be provided with an easy one-click method of doing so in their email client.

Businesses should also ensure they have advanced anti-spam software with email sandboxing and URL filtering, and have multifactor authentication set up for all email accounts, with phishing-resistant multifactor authentication implemented when possible for the greatest protection.

Microsoft Teams Used in Tech Support Scam Targeting Female Executives

by G Hunt | April 28, 2025 | Security Awareness

A new campaign has been identified that abuses Microsoft Teams to deliver malware in a tech support scam, where the user is tricked into believing they need assistance to resolve a technical issue that requires them to grant access via the built-in Microsoft remote monitoring and management tool, Windows Quick Assist.

Tech support scams are a very common form of cybercrime. According to the FBI's Internet Crime Complaint Center (IC3), 36,002 complaints were received about tech support scams in 2024, making it the 6th most commonly reported cybercrime, and the third biggest cause of losses, with more than $1.46 billion lost to the scams in 2024 alone. It should be noted that many victims fail to report these scams to the FBI, so the number of victims and the losses are likely to be substantially higher.

While the companies impersonated are highly varied, these scams typically involve contact being made with the victim, with the scammer impersonating a member of the technical support team to resolve a fictitious technical

issue. To make these scams more realistic, threat actors may add a targeted individual to numerous newsletters and spam sources, and then call to help them resolve the spam problem that the threat actor has created.

One of the latest scams saw contact made via Microsoft Teams on targets in the services sector, including finance, professional, and scientific services. One common denominator was that the targeted individuals all had female-sounding names, most of whom were executive-level employees. The scam was also conducted at specific times, between 2 p.m. and 3 p.m. local time, which the threat actors perceived would be the ideal time when attention would likely be reduced and the scam was most likely to succeed.

The Teams request was accompanied by a vishing call. Over the phone, the target was convinced to run a PowerShell command that was delivered via a Microsoft Teams message, which downloaded the first-stage payload. The QuickAssist tool was used by the threat actor for remote access to ensure the deployment of PowerShell, all under the guise of resolving a fictitious technical issue.

The threat actor used QuickAssist to deliver a signed file named Team Viewer.exe to a hidden folder, with that executable likely to be undetected as it would be hidden in normal system activity. The file was used to sideload a malicious DLL called TV.dll, which was used to deliver a second-stage JavaScript-based backdoor, providing persistent access to the user's device. Persistence was achieved by modifying Registry entries. The campaign was identified by a ReliaQuest researcher and was attributed to a tracked threat actor that uses vishing attacks to infect users with malware, often leading to a ransomware attack. One method of blocking these attacks is to configure Microsoft Teams to block external communications to prevent the initial contact, and if Windows Defender is used, to set it to the most restrictive setting to limit the use of PowerShell.

Ultimately, this scam succeeded because an end user was contacted, and social engineering techniques were used to trick them into taking the actions that the threat actor could not otherwise have performed externally. The recently published Verizon Data Breach Investigations Report revealed that 60% of data breaches involved the human element, with social engineering one of the most common ways that employees are tricked. It is not necessary for threat actors to spend countless hours trying to find zero-day vulnerabilities in software solutions when they can just contact employees and get them to provide the access they need.

As the IC3 data shows, these scams are lucrative for threat actors, and one of the reasons why they are so successful is that they tend to take place over the phone, bypassing the need to defeat anti-spam software and other technical security measures. Since legitimate remote access tools are used, the malicious activity is easy to hide within normal system activity.

Security awareness training can go a long way toward improving defenses against these types of scams. Executives were targeted in this campaign as they have higher-level privileges than other workers, but security awareness training is often less robust at the executive level. It is important to ensure that all members of the workforce,e from the CEO down, are provided with security awareness training, and for the training courses to be tailored to different roles and the specific threats that each is likely to encounter.

With the SafeTitan security awareness training platform, it is easy to create tailored training programs for different members of the workforce and the unique threats that they face, including specific programs for the CEO and executives, the HR department, and the IT team. With the SafeTitan platform, there are hundreds of training modules tailored to different aspects of cybersecurity and different threats, making it quick and easy to create and

deliver highly effective training courses covering phishing and other email-based attacks, smishing, vishing, and other cyber threats.

Give the TitanHQ team a call today for more information on improving your cybersecurity defenses and security awareness training programs. All TitanHQ solutions are available on a free trial, with support provided to make sure you get the most out of your trial.

The Human Element is Involved in 60% of Data Breaches

by G Hunt | April 26, 2025 | Phishing & Email Spam

The latest data from Verizon has revealed that phishing was the third most common method of initial access in the data breaches the firm analyzed for its 2025 Data Breach Investigations Report. Phishing accounted for 16% of all data breaches in 2025, having been overtaken by vulnerability exploitation (20%). The leading initial access method was credential misuse, which was involved in 22% of data breaches. Verizon does note, however, that while incident responders may identify compromised credentials as the cause, it is not always clear how those credentials were obtained. It is possible that they were obtained in a previous phishing attack that went undetected, so phishing may have been involved in a higher percentage of data breaches.

The report highlights the extent to which cybercriminals exploit human weaknesses. The human element was involved in approximately 60% of data breaches in 2024, down slightly from the 61% of data breaches the previous year. The human element could involve a click on a link in a phishing email, resulting in the theft of credentials, a visit to a malicious website where malware is downloaded, a misconfiguration that is exploited, or a response to a phone call or text message. In 32% of data breaches, the human element was ascertained to result in credential abuse, 23% involved social interactions, 14% involved errors, and 7% involved interactions with malware.

This year’s report delves into the importance of security awareness training and how providing regular training can really make a difference to an organization’s security posture, especially when combined with phishing simulations. Providing training to the workforce will teach employees about security best practices, which will help to eradicate risky behaviors. Employees should be taught how to identify a phishing email and be conditioned to report any suspicious emails to their security team immediately. Phishing simulations help to reinforce training and identify individuals who have failed to apply the training. If an individual fails a phishing simulation, they can be provided with additional training to help ensure they do not make a similar identification error in the future.

The report revealed that out of the companies that provided security awareness training and conducted phishing simulations, there was a much higher reporting rate when employees had received training more recently. The baseline reporting rate was 5%, which shot up to 21% with recent training.

The data shows why it is so important to provide ongoing security awareness training to keep cybersecurity matters fresh in the mind. It is also important to incentivize employees to report potential phishing emails rather than punish those who don’t, and to clearly explain that reporting suspicious emails helps security teams to contain threats more quickly and limit the damage. It is also important to make it as easy as possible for employees to report potential threats. Ideally, employees should be able to report a potential phishing or scam email with a single click in their email client.

TitanHQ offers an email security suite that includes the SpamTitan cloud-based anti-spam service and the PhishTitan phishing prevention and remediation solution for Microsoft 365 users. SpamTitan incorporates dual anti-virus engines for detecting known malware, email sandboxing for detecting novel threats, AI and machine-based learning algorithms for identifying phishing and spam emails, plus SPF, DKIM & DMARC, allow listing, blocking, greylisting, and dedicated real-time block lists. An email client add-in is also provided to allow employees to easily report potential threats.

The PhishTitan solution is based on the same engine that powers SpamTitan, incorporating AI and machine learning to detect phishing threats, and also adds banner notifications for emails to warn employees about potential threats from external email addresses. The remediation tools provided by PhishTitan allow security teams to rapidly respond to threats and eliminate them from their email system.

Both email security solutions have high detection accuracy and provide best-in-class protection from email threats. In recent independent tests at VirusBulletin, the solutions were demonstrated to have exceptional detection accuracy, blocking in excess of 99.99% of spam and phishing threats, and thanks to the email sandbox service, TitanHQ's solutions blocked 100% of malware.

TitanHQ can also help with security awareness training and phishing simulations. The SafeTitan platform makes it easy to create and automate continuous security awareness training programs for the workforce. The training content is enjoyable and interactive and is delivered using computer-based training, with individual modules taking no more than 10 minutes to complete.

The training content is regularly updated and has been proven to improve security awareness and reduce susceptibility to cyber threats, especially when combined with TitanHQ's phishing simulator. Internal simulated phishing campaigns can be created and automated, and will automatically generate additional training immediately in response to a security failure, ensuring training is delivered at the time when it is most likely to be effective.

Through security awareness training and phishing simulations, organizations can reduce the employee errors that cause so many data breaches, and by using TitanHQ's email security suite, threats will be blocked before employees' security awareness is put to the test.

Give the TitanHQ team a call today to discuss the best options for improving your defenses. All TitanHQ solutions are available on a free trial and assistance can be provided to help you get the most out of the free trial.

UK Government Survey Confirms Phishing is the Biggest Threat to UK Businesses

by G Hunt | April 25, 2025 | Phishing & Email Spam

A recently published report commissioned by the UK's Home Office and Department for Science Innovation and Technology (DSIT) has revealed that 43% of UK businesses and 30% of UK charities experienced a cybersecurity breach in the past 12 months.

While there was a slight fall in the number of businesses and charities suffering a cybersecurity incident, there was a significant increase in ransomware attacks. The survey was conducted on 2,180 businesses, 1,081 charities, and

574 educational institutions. Based on the number of confirmed cyber incidents, that equates to around 612,000 UK businesses and 61,000 UK charities experiencing a cyber breach or a cyberattack in the past 12 months.

While there was a slight decline in cyber incidents, which were confirmed by 50% of businesses in last year's study, it is clear that hacking and other types of cyber incidents continue to pose a massive threat to UK businesses, with ransomware attacks of particular concern. According to the report, the estimated percentage of ransomware crime increased from less than half a percent in 2024 to 1% in 2025, which suggests that around 19,000 UK businesses experienced a ransomware incident in the past 12 months. 4% of large businesses and 3% of medium-sized businesses admitted to paying the ransom demand to recover their data and prevent its publication online.

The biggest cyber threat to UK businesses by some distance is phishing. Phishing is the fraudulent practice of sending emails or other messages that trick individuals into disclosing sensitive information such as login credentials or installing malware. Over the past 12 months, 93% of businesses and 95% of charities that experienced a cybercrime incident identified phishing as the cause of at least one of those incidents. Businesses that were confirmed victims of cybercrime in the past 12 months experienced an average of 30 cybercrime incidents in the past 12 months, with charities experiencing an average of 16 cybercrime incidents.

The credentials stolen in these attacks and the malware installed give cybercriminals initial access to internal networks. From there, they can deploy additional malware payloads and ransomware and steal sensitive data. The phishing problem is also getting worse for businesses, as cybercriminals are leveraging large language models (LLMs) to craft extremely convincing phishing emails and conduct phishing attacks at scale. These tools can be used to generate fake images, make phishing lures more believable, and make them harder to detect.

With phishing such a major threat and the high cost of dealing with each phishing incident, UK businesses and charities need to have email security defenses capable of detecting and blocking phishing threats, including those developed using AI and LLMs.

Phishing defenses should consist of anti-spam software, multifactor authentication, and end user security awareness training as a minimum. Advanced email filtering software incorporates antivirus software to identify known malware threats, email sandboxing for detecting novel malware threats, link scanning, and machine learning and AI-aided detection.

Over the past three quarters, SpamTitan from TitanHQ has consistently demonstrated in independent tests that it is capable of blocking even the most advanced threats, routinely achieving a 100% malware detection rate, and phishing and spam detection rates in excess of 99.99%.

TitanHQ also offers a comprehensive security awareness training and phishing simulation platform – SafeTitan – for improving awareness of cyber threats. When combined with phishing simulations, the platform has been shown to reduce employee susceptibility to phishing by up to 80%. The training content is enjoyable and memorable, and is delivered in training modules of no more than 10 minutes to maximize knowledge retention and make training easy to fit into busy workflows.

All TitanHQ solutions have been developed to provide powerful protection and advanced features, while also being easy to set up, configure, and use. Further, they are available at a price point that is affordable for businesses

of all sizes. Give the TitanHQ team a call today to find out more about improving your defenses against phishing and other cyber threats. Further, TitanHQ's cloud-based anti-spam service and security awareness training platform are available on a free trial, allowing you to put them to the test before making a purchase decision.

Wine-Tasting Phishing Emails Used to Target Embassy Staff in Malware Campaign

by G Hunt | April 24, 2025 | Phishing & Email Spam

A phishing scam has been identified targeting staff of European embassies with an invitation to a fake wine-tasting event. Targets include European diplomats and the staff of non-European countries at embassies located in Europe. The campaign has been linked to the Russian state-sponsored hacking group, Cozy Bear (aka APT29, Midnight Blizzard), and is believed to be primarily an espionage campaign.

The aim of the campaign is to deliver a stealthy new backdoor malware dubbed GrapeLoader. The campaign, identified by Check Point, is believed to be part of a wider campaign targeting European governments, diplomats, and think tanks. The malware delivered in the campaign serves as a loader for delivering additional payloads and is used as an initial stage tool for fingerprinting and establishing persistence.

As is typical with spear phishing campaigns, considerable effort has been put into creating a lure that is likely to elicit a response. A fake diplomatic event is used, commonly related to wine tasting, with some emails offering a place at a diplomatic dinner. The messages were sent by a specific individual at a legitimate but impersonated European foreign affairs ministry. A series of follow-up messages is sent to individuals who failed to respond to the fake invite. The phishing link is also configured to redirect the user to the real foreign ministry website if it is opened outside of the expected timezone or by an automated tool.

The emails prompt the recipient to click on an embedded hyperlink that directs them to a spoofed website where they are prompted to download a file. If successful, the user downloads a zip file containing a PowerPoint executable file called wine.exe, and two hidden DLL files, one of which allows the PowerPoint file to run. The PowerPoint file is used for DLL sideloading, including the other DLL file, dubbed GrapeLoader, which is used to deliver additional payloads. GrapeLoader fingerprints the device and establishes contact with its command-and-control server. A Run registry key is added to ensure that wine.exe is executed following a reboot.

The malware has been designed to be stealthy, including masking strings in its code and only decrypting them for a short time in the memory before they are erased. This technique prevents analysis using tools such as FLOSS. The malware also makes memory pages temporarily inaccessible to evade antivirus scans. GrapeLoader is thought to lead to the delivery of a modular backdoor known as WineLoader, which has been used in previous Cozy Bear campaigns on governments and political parties.

GetShared and Other Legitimate Services Abused in Phishing Campaigns

by G Hunt | April 22, 2025 | Phishing & Email Spam

One of the common tactics for getting phishing emails into inboxes is to use a legitimate service to send the emails, as the messages are far less likely to be blocked by email security solutions. Email security solutions

perform reputation checks on email addresses and domains, and if they are determined to have been used for spamming or sending malicious emails, they are rapidly added to real-time blocklists (RBLs). If a certain trustworthiness threshold is exceeded, the messages will be blocked and quarantined, ensuring they do not reach their intended targets.

These reputation checks are often passed if emails are sent via trusted services such as Dropbox and Google Calendar, and similarly if malicious files or content are hosted on legitimate services such as OneDrive, GitHub, Google Drive, or SharePoint. The fact has not been lost on threat actors, who regularly abuse these services.

Fake login pages may be hosted on cloud storage services, and malicious files shared through them. Not only can these emails evade checks due to the good reputation of the sites, these well-known brands are familiar to end users and are often trusted, increasing the probability that credentials will be divulged or files will be downloaded.

For instance, a recent campaign abusing Dropbox used the platform to send an email about a shared file, which was also hosted on a legitimate Dropbox account. The email contained a link to a malicious PDF file, branded with the details of a company known to the targeted employees. The PDF file contained a link to another, unrelated website, where a malicious file was hosted. The phishing emails used a plausible lure to convince the user to click the link and download and execute the file.

A new campaign has recently been identified that uses a different legitimate service to evade reputation checks. The campaign, detected by security researchers at Kaspersky, was sent via a service called GetShared. While not as well-known as Google Calendar or Dropbox, the platform had a vulnerability that could be abused to send emails from a trusted domain and file-sharing service.

Similar to the Dropbox campaign, GetShared was used to send an email to targeted individuals advising them that a file had been shared with them via GetShared, as it was too large to send via email. The use of the file-sharing service seems reasonable, and the urgency was believable. The user was told that the file would be deleted after a month, and they were asked to provide a quote including the delivery time and payment terms. One of the intercepted emails targeted a designer using a shared file called DESIGN LOGO.rar.

The user was given a download button, which links to the site where the file can be downloaded. If the compressed file is opened and the contents extracted, there are several possible attack methods. An executable file could be in the compressed file that has a double file extension, making it likely that the file would be executed. Potentially, the file could contain a link to a malicious document or phishing page, although in this case, it was part of a vishing campaign. The compressed file contained contact details for the user to call, which would require a file download or disclosure of credentials or other sensitive information.

Earlier this year, a campaign was identified that used Google Calendar, with the emails sent through the platform containing a calendar invite. The invite is automatically added to the user’s Google Calendar account if they have Calendar set up and configured to automatically accept invitations. The invite contained a link to Google Forms or Google Drawings, which contained a link to a phishing website. That website impersonated a well-known brand and required the user to log in with their credentials. The campaign targeted more than 300 brands including healthcare providers, educational institutions, banks, and others, and involved thousands of emails.

Traditional email security solutions are unlikely to block emails from these trusted senders, and malicious files hosted on trusted platforms are also unlikely to be blocked. Businesses can combat these types of phishing attacks by using advanced email spam filter that incorporates AI and machine learning algorithms and email sandboxing in addition to the standard reputation checks and blacklists. The best spam filters for businesses provide multiple layers of protection to block these malicious emails and prevent them from reaching inboxes; however, due to the difficulty in distinguishing genuine from malicious communications from legitimate platforms, security awareness training is vital.

Employees should be trained on how to identify phishing emails and told not to trust emails from legitimate platforms, as while the platforms can be trusted, the content cannot. It is also recommended to use a phishing simulator to run simulations of phishing using lures that abuse trusted platforms to gauge how employees respond and provide targeted training to individuals who are tricked by these campaigns.

SocGholish Malware Used to Deliver RansomHub Ransomware

by G Hunt | March 31, 2025 | Internet Security, Phishing & Email Spam, Security Awareness

RansomHub is one of the most prolific ransomware-as-a-service (RaaS) groups now that the ALPHV/BlackCat operation has shut down and the LockBit operation has been hit with successive law enforcement actions. RansomHub engages in double extortion tactics, exfiltrating sensitive data from victims' networks and encrypting files. Victims must pay to obtain the keys to decrypt their data and to prevent the publication of the stolen data on the RansomHub data leak site. Since emerging in early 2024, the group has conducted more than 200 attacks.

As a RaaS operation, RansomHub uses affiliates to conduct attacks in exchange for a percentage of any ransom payments they generate. The affiliates each have their specialties for breaching victims' systems, including phishing, remote desktop protocol attacks, and the exploitation of unpatched vulnerabilities. Now, a new tactic is being used – The group is using the SocGholish malware-as-a-service (MaaS) framework for initial access, especially in attacks on the government sector.

SocGholish, also known as FakeUpdates, uses an obfuscated JavaScript loader that is primarily delivered via compromised legitimate websites. After compromising a website, malicious scripts are added that redirect users to webpages that display browser update notifications. These sites use social engineering to trick visitors into downloading a browser update, as they are told that their browser has a security issue or is not functioning correctly. If the user agrees, they download a zip file that contains a JavaScript file. If that file is executed, SocGholish malware is installed.

SocGholish is a malware downloader that provides initial access to a victim's network. The malware has been used to deliver a wide range of payloads, including AZORult, Gootloader, NetSupport, and Dridex. SocGholish has also previously been used to deliver DoppelPaymer ransomware, and now RansomHub ransomware. In the case of RansomHub, the group deploys Python-based backdoor components for RansomHub affiliates to use for initial access.

Preventing SocGholish infections is critical to preventing RansomHub ransomware attacks; however, prevention requires a defense-in-depth approach. Traffic to the compromised websites can come from emails that include embedded hyperlinks, malvertising, SEO poisoning, and links to compromised websites are also delivered to users

via Google Alerts. The webpages that host the fake browser updates filter traffic, blocking access by sandboxes, which can make detection difficult.

The best approach is to use an advanced anti-spam software such as SpamTitan to block malicious emails. In the last quarterly round of testing at VirusBulletin, SpamTitan, a cloud-based antispam service from TitanHQ, ranked #1 for malware detection, phishing detection and spam blocking with a 0% false positive rate, and in the February 2025 tests, achieved a perfect score blocking 100% of malware, phishing, and spam emails. The high detection rate is due to extensive front-end tests, email sandboxing, and machine learning.

A web filter adds an important layer of protection by scanning websites for malicious content and blocking access to known malicious websites. The WebTitan DNS filter is fed extensive threat intelligence to block access to known compromised webpages, can filter websites by category, and can be configured to block downloads of executable files from the Internet. Security awareness training is vital for creating a human firewall. Employees should be informed about the risks of interacting with security warnings on the Internet, and taught how to identify phishing attempts and be instructed on security best practices. The SafeTitan security awareness training platform and phishing simulator platform make creating and automating training courses and phishing simulations a quick and easy process.

QR Code Phishing Scam Requests Verification of Tax Information

by G Hunt | March 31, 2025 | Phishing & Email Spam

One of the ways that cybercriminals are bypassing traditional email security solutions is to use QR codes rather than embedded hyperlinks in their phishing emails. QR codes are increasingly used by businesses to drive traffic to web pages, as consumers do not need to go through the process of typing a URL into their browser. The QR code can simply be scanned with a smartphone camera, the URL will be recognized, and the web resource can be visited with a single tap of the finger.

Spam filtering services will detect links in emails, check them against blacklists of known malicious websites, and will often follow the links to find the destination URL. If the website is malicious, the email will not be delivered to the user's inbox. By using a QR code rather than a hyperlink, there is an increased chance that the message will be delivered, as many anti-spam software solutions are incapable of reading QR codes.

One such campaign has recently been identified that warns the recipient that they must review and update their tax records. The email has the subject, "urgent reminder," and claims to have been sent by the Tax Services Team. The email has a PDF file attachment and advises the recipient that a review of their tax records must be completed by April 16, 2025, to avoid potential penalties. Tax season is well underway and annual tax returns need to be submitted by April 15, 2025, so the deadline for a response is plausible.

Rather than include a link, the PDF file includes a QR code, which the user is told they should scan with their mobile device to access the secure tax portal, where they must log in, review their tax information, and confirm it is up to date.

If the QR code is scanned and the link followed, the user must first pass a CAPTCHA test, after which they are presented with a Microsoft login prompt and asked to enter their password. The form is already populated with the

user's email address to make it appear that the user is known or has visited the site before, adding an air of legitimacy to the scam. If the password is entered, it will be captured and used to hijack the user's Microsoft account. After entering the password, the user is told "We could not find an account with that username. Try another account," which may allow the attacker to steal credentials for another account.

QR code phishing forces users onto a mobile device, which typically has weaker security than a desktop computer or laptop, plus only the domain name can usually be viewed rather than the full URL, which helps to make the link seem legitimate. Phishers also often use open redirects on legitimate websites to make their links appear authentic and hide the final destination URL.

With QR code phishing scams on the rise, it is important to raise awareness of the threat through your security awareness training program. Employees should be warned that QR codes are commonly used by threat actors, and never to follow links encoded in QR codes that arrive via email. It is also recommended to use a phishing simulator to assess whether the workforce is susceptible to QR code phishing attempts. The SafeTitan security awareness training platform allows businesses to easily conduct phishing simulations on the workforce to gauge susceptibility to phishing threats. The phishing simulator will generate relevant training content immediately if a phishing test is failed, ensuring targeted training content is delivered immediately, when it is likely to be most effective at correcting behavior.

Technical defenses should also be implemented. An advanced spam filtering service should be used that is capable of identifying QR codes and following and assessing URLs for phishing content and malware. The outbound spam filter of SpamTitan is capable of following QR codes and assessing content, and in recent tests, correctly identified 100% of phishing attempts. SpamTitan also includes email sandboxing for in-depth analysis of email attachments. A DNS security solution is also recommended for in-depth analysis of URLs for malicious content to provide an extra layer of protection against phishing and malware.

New Phishing Kit Dynamically Displays Relevant Landing Pages Based on DNS Queries

by G Hunt | March 30, 2025 | Phishing & Email Spam

A new phishing-as-a-service (PhaaS) platform has been identified that highlights the sophistication of phishing attacks, and how even cybercriminals with limited skill sets can conduct extremely effective phishing campaigns.

One of the problems when conducting phishing campaigns is ensuring the phishing emails are convincing. Phishing has traditionally been a numbers game, where large volumes of messages are sent in the knowledge that a small number of individuals will be tricked into responding. Those individuals may simply be busy and respond without taking the time to carefully consider what they are being asked, or individuals with poor security awareness. Targeted phishing attempts, termed spear phishing, involve research and are tailored to individuals or small numbers of individuals, and because of the targeting, there is a much higher response rate. The trade-off is that these campaigns involve considerable time and effort.

The new PhaaS platform allows a threat actor to tailor the content to display a fake login page relevant to the individual receiving the message, while still sending a large volume of phishing emails. The phishing kit allows individuals to be tricked by displaying a login prompt that impersonates any of 114 brands in around a dozen

different languages, with the content displayed tailored to each individual. The threat actor configures the phishing campaign, sends out phishing emails via the PhaaS kit, and the link in the email directs the recipient to a phishing webpage. The next stage is where the targeting occurs. The threat actor queries the email domain DNS MX records (DNS over HTTPS) obtained from Cloudflare or Google to identify the user's email service provider. The phishing page is then dynamically displayed based on the results of that query, and if no response is received, the phishing page defaults to Roundcube.

DNS queries are fast, so the query and response occur in a fraction of a second, as is the case when a DNS query is sent to identify the IP address of a webpage when browsing the internet. As such, there is only a very small delay, often unnoticeable to the user, before the content is loaded. The result is that if the user's email service provider is Gmail, they will be presented with a Gmail login prompt, and if they use Microsoft Outlook, they will be presented with a Microsoft login prompt. If the user responds and enters their login credentials, they are captured and sent to the collection server, and the user is redirected to the real login page for that service, most likely unaware that they have been phished. The phishing campaign was identified by InfoBlox, which identified thousands of phishing emails sent via the kit. While the kit appears to have been first used in 2020, since then the number of brands being impersonated has increased considerably, with support also provided to target users in several languages.

The phishing kit demonstrates the sophistication of phishing attacks and how threat actors are increasing the effectiveness of their campaigns. Businesses should respond to the evolving threat landscape by adopting a defense-in-depth approach that includes a DNS filtering solution such as WebTitan, advanced spam filtering software such as SpamTitan, and ongoing security awareness training and phishing simulations for the workforce to raise awareness of threats and reduce susceptibility to phishing attempts, using a solution such as SafeTitan.

Fake Browser Update Campaign Delivers FrigidStealer Malware to Mac Users

by G Hunt | March 4, 2025 | Phishing & Email Spam, Spam Software, Website Filtering

There has been a surge in infostealer malware infections, with detections up almost 60% from the previous year. Infostealers gather system information, stored files, and sensitive data and exfiltrate the information to their command and control server. Once installed, they can remain undetected for long periods of time, exfiltrating sensitive data such as usernames and passwords by logging keystrokes, with some variants capable of taking screenshots and capturing audio and video by taking control of the microphone and webcam.

The majority of infostealers are used to attack Windows systems; however, a new infostealer called FrigidStealer has been identified that is being used to target Mac users. FrigidStealer is capable of stealing saved cookies, password-related files in the Safari and Chrome browsers, and login credentials, along with cryptocurrency wallet credentials, Apple Notes containing passwords, documents, spreadsheets, text files, and other sensitive data from the user's home directory. The gathered data is added to a compressed file in a hidden folder in the user's home directory and is exfiltrated to its command and control server.

The threat actor behind the campaign distributes FrigidStealer under the guise of important web browser updates on compromised websites. The threat actor injects malicious JavaScript into the HTML of the webpage which

generates a fake browser update notification to website visitors. The notifications warn the user that they must update their browser to continue to view the page, with the displayed notification tailored to the browser in use.

The notifications look professional, include the appropriate logos for either Google Chrome or Safari, and contain an update button that the user must click to proceed. Clicking the button will trigger the download of an installer (DMG file), which must be manually launched. The user is required to enter their password to get around macOS Gatekeeper protections. If the password is entered, the file is executed and FrigidStealer is delivered.

A similar campaign is being conducted targeting Windows users. The Windows campaign uses similar techniques, although it tricks the user into downloading and executing an MSI installer, which delivers one of two different info stealers, Lumma Stealer or DeerStealer. The threat actor is also targeting Android devices in a similar way, delivering an APK file that contains the Marcher banking Trojan.

With infostealer infections soaring, businesses need to make sure they have the right security solutions in place and should be providing regular security awareness training to the workforce. Employees should be instructed to never download browser updates when prompted to do so on websites or run any suggested commands on their devices, as the updates and commands are likely to be malicious.

A web filter is strongly recommended for controlling access to the Internet and blocking visits to malicious websites. The WebTitan DNS filter can used to protect users on or off the network and is constantly updated with threat intelligence on new malicious websites. If an attempt is made to visit a known malicious website, that attempt will be blocked. The web filter can also be configured to block file downloads from the internet by file type, allowing IT teams to prevent employees from downloading executable files.

While this is a web-based campaign, information stealers are commonly distributed in phishing emails, either through malicious attachments or embedded hyperlinks. TitanHQ's SpamTitan cloud-based anti-spam service is a powerful AI-driven email security solution with email sandboxing and advanced threat detection capabilities. SpamTitan outperformed all other tested solutions in recent tests by VirusBulletin, blocking 100% of phishing emails and 100% of malware.

That Google Chrome Installer May be Malware!

by G Hunt | February 28, 2025 | Security Awareness, Website Filtering

A China-based ransomware group, Silver Fox, that has primarily targeted individuals in China, Taiwan, and Hong Kong, has been expanding its attacks outside of those regions and is now conducting attacks more broadly on multiple industry sectors. Silver Fox uses ransomware in its attacks and is focused on file encryption, demanding payment to obtain the keys to decrypt files. While the group does engage in double extortion tactics, stealing data and threatening to leak that data if the ransom is not paid, data theft is limited. Highly sensitive data is not generally stolen.

Many ransomware groups breach networks and spend time moving laterally to infect the maximum number of devices possible and also spend time locating sensitive data to exfiltrate. It is often the data theft and threat of publication that is the main driver behind ransom payments, so much so that some ransomware groups have abandoned the file encryption element of their attacks. In contrast, Silver Fox is focused on quick attacks, often

breaching networks and encrypting files on the same day. The group even abandons attacks if lateral movement is not possible or if strengthened security is encountered.

Silver Fox primarily gains initial access to victims' networks by deploying a remote access Trojan called ValleyRAT. ValleyRAT was first identified in 2023 and is believed to be a malware tool developed by Silver Fox, and its function is to give Silver Fox remote access to networks. The group has extensively targeted individuals in accounting, finance, and sales since those employees are likely to have access to sensitive data that can be quickly and easily stolen.

ValleyRAT is delivered by multiple means, indicating Silver Fox is trying to infect as many users as possible. One of the main methods used for distribution is fake installers for popular software. For instance, the group has been observed using fake installers for EmEditor (a Windows text editor), DICOM software (for viewing medical images), and system drivers and utilities. The group has also been observed using a spoofed website offering the Google Chrome browser, which prompts the user to download a ZIP file containing a Setup.exe file, which installs ValleyRAT.

The methods used to drive traffic to these fake downloads are unclear, although traffic to the fake Google Chrome download site is thought to be generated through malvertising and SEO poisoning, where malicious adverts are displayed for key search terms related to Chrome and web browsers that redirect users to the drive-by download site. SEO poisoning may be used, where black hat SEO techniques are used to get web pages to appear in the search engine listings for key search terms. If the user is tricked into executing the fake installer, they will be infected with ValleyRAT and a ransomware attack will rapidly follow.

Since the group is focused on rapid attacks involving minimal effort, the best defense is to strengthen baseline security and make lateral movement difficult through network segmentation. To prevent ValleyRAT downloads, web security needs to be improved to block attempts by users to visit the malicious websites. A web filter is an ideal tool for blocking access, including redirects through malvertising and SEO poisoning. A web filter such as WebTitan can also be configured to block downloads of certain files from the Internet and restrict access to websites by category – software download sites for example. Ongoing (and regular) security awareness training is also vital to teach employees about the risk of downloading software from the Internet, raise awareness of phishing, and teach security best practices, adding an important human layer to your security defenses.

TitanHQ's web filter, WebTitan, is easy to implement and use, is automatically updated with the latest threat intelligence, and provides exceptional protection against web-based threats. When coupled with the SafeTitan security awareness training and phishing simulation platform, businesses will be well protected against ValleyRAT malware and other web-delivered malware payloads. Give the TitanHQ team a call to discuss these and other cybersecurity solutions to better protect you against the growing malware threat.

Researchers Confirm Massive Threat From Information Stealing Malware

by G Hunt | February 27, 2025 | Phishing & Email Spam, Security Awareness, Spam Software

Cybercriminals have extensively used ransomware in their attacks on businesses, government entities, and critical infrastructure, and while these attacks often make headline news and cause massive disruption, there is a much more common malware threat – Information stealers.

Information stealers are malware that is silently installed on devices that can remain undetected for long periods of time. These types of malware have many different capabilities and can serve as downloaders for other malicious payloads, but their main function is information theft. Information theft is achieved in several ways, depending on the malware variant in question. These malware types often have keylogging capabilities and can record keystrokes as they are entered on the keyboard, allowing sensitive information such as usernames and passwords to be captured. They can often record audio from the microphone, take control of the webcam and record video, and take screenshots. They can also steal browser histories, cookies, and other sensitive information.

The information stolen from the victim allows the threat actor to conduct follow-on attacks, access accounts and steal further sensitive data, access and drain financial accounts, or commit identity theft and other types of fraud. Information stealers can also provide a threat actor with access to a device, and that access is often sold to specialized cybercriminal groups such as ransomware actors. Many hackers now act as initial access brokers, using information stealers to gain access before selling that access to other cybercriminal groups.

Information stealers such as Lumma, AgentTesla, FormBook, Redline, and StealC have been increasingly used in recent years, especially last year. Check Point observed a 58% increase in attacks from the previous year, and a report from the threat intelligence firm KELA suggested that lists of credentials obtained from information stealers are being shared on cybercrime forums. The credential lists included billions of logins that had been captured from infected devices, which, according to KELA, included around 4.3 million devices, of which around 330 million credentials had been stolen. An estimated 40% were corporate credentials.

The breach notification service, Have I Been Pwned (HIBP), has recently added 284 million compromised accounts to the service. The credentials were identified from chats on a Telegram channel called ALIEN TXTBASE, with the data obtained from information stealer logs. HIBP founder Troy Hunt said the stealer logs included 23 billion rows of data with 493 million unique website and email address pairs and around 284 million unique email addresses. Hunt said 244 million passwords were not previously known to the HIBP service, with 199 million already in its database.

The extent to which these malware variants are used, and the increase in use in 2024, clearly demonstrates the importance of advanced malware protection and the sheer number of compromised credentials suggests many businesses have been infected with information stealers. The problem for businesses is that these malware variants can be difficult to identify, as new versions are constantly being released. Traditional antivirus software is signature-based, which means it can only detect known malware. When new malware is identified, a signature of that malware is obtained and fed into antivirus software. If a malware signature is not in the software's definition list, it will not be detected. There are several ways that these information stealers are distributed, with email being one of the most common. They can also be downloaded from the internet from malicious websites in drive-by downloads or installed along with pirated software or doctored versions of legitimate software installers.

Defending against information stealers requires a combination of measures – a defense-in-depth approach, with multiple overlapping layers of security. Given the high volume of infections stemming from email, businesses need a spam filter to block malicious emails. Antispam software will block many malicious emails; however, an antispam server must have advanced antimalware defenses. That means traditional signature-based detection and advanced behavioral detection to ensure previously unseen malware is identified and blocked.

SpamTitan uses dual anti-virus engines for detecting known threats and a next-generation email sandbox for behavioral analysis. If standard checks are passed, suspicious messages are sent to the sandbox – a safe environment where they are detonated and their behavior is analyzed. This vastly improves the detection rate, and in recent independent tests, SpamTitan outperformed all other tested email security solutions and had a 100% malware detection rate.

Security awareness training needs to be provided to the workforce to ensure that employees have the skills to recognize and avoid threats, no matter where they are encountered. Through training, employees should be conditioned to always report potential threats to their security team, and businesses can promote security best practices and eradicate risky behaviors. TitanHQ offers businesses a comprehensive training and phishing simulation platform – SafeTitan – that has been shown to be highly effective at improving employees' security awareness.

Many malware infections occur via the Internet, and while training can reduce risk, a technical security solution is required to block threats. WebTitan is a DNS-based web filter that is used to block access to known malicious websites, assess websites in real-time for malicious content, block certain file downloads from the Internet, and restrict the sites and web pages employees can access.

With these three security solutions in your arsenal, you will be able to significantly improve your security posture and block information stealers and other threats. Give the TitanHQ team a call today to find out more or take advantage of a free trial of these solutions.

Smishing and Vishing Used by Ransomware Group for Initial Access to Corporate Networks

by G Hunt | February 26, 2025 | Phishing & Email Spam, Security Awareness, Website Filtering

A ransomware group called EncryptHub has been accelerating attacks and is now known to have breached the networks of more than 600 organizations worldwide. EncryptHub has been active since June 2024 and gains initial access to victims' networks via spear phishing attacks, with initial contact made via SMS messages rather than email.

The group impersonates commonly used corporate VPN products such as Palo Alto GlobalProtect and Cisco AnyConnect as well as Microsoft 365, and drives traffic to its malicious domains by making contact via personalized SMS messages (smishing) or the phone (vishing).

If vishing is used and the victim is contacted by phone, EncryptHub impersonates a member of the IT helpdesk and uses social engineering techniques to trick them into disclosing their VPN credentials. The phone number is spoofed to make it appear that the call is coming from inside the company or Microsoft Teams phone numbers are used. The victim is told that there is a problem with the corporate VPN that needs to be resolved, and if the scam works, the user is sent a link via SMS that directs them to a domain that resembles the VPN solution used by that company. If the user enters their credentials, they are used in real-time to log in, and if there are any multifactor authentication prompts, the threat actor is able to obtain them on the call. After successfully gaining access, the user is redirected to the genuine login page for their VPN, and the call is terminated.

Another tactic used by the group involves SMS messages with a fake Microsoft Teams link with the goal of capturing their Microsoft 365 credentials. The user is directed to a Microsoft Teams-related login page and the threat actor exploits Open URL parameters on microsoftonline.com to harvest email addresses and passwords, while the user believes they are interacting with the legitimate Microsoft service. Once access is gained, the group uses PowerShell scripts and malware to gain persistence, then moves laterally, steals data, deploys the ransomware payload, and issues a ransom demand.

The group's tactics are highly effective, as in contrast to spear phishing via email, it is difficult to block the initial contact via SMS or over the phone. The key to preventing these attacks is improving the security awareness of the workforce and using a web filter to prevent the phishing domains from being accessed by employees. TitanHQ's web filter, WebTitan, is a DNS-based web filtering solution that is constantly updated with the latest threat intelligence from multiple sources to provide up-to-the-minute protection against new phishing domains. Any attempt to visit a known phishing domain or other malicious site will be blocked, with the user directed to a locally hosted block page.

Regular security awareness training for the workforce is vital to teach security best practices and raise awareness of the tactics used by cybercriminals to breach corporate networks. With the SafeTitan security awareness training platform, businesses can easily create training programs tailored for individuals, roles, and departments, and automate those campaigns so they run continuously throughout the year, delivering training in small chunks on a weekly or monthly basis. It is easy to incorporate new training in response to changing threat actor tactics to increase awareness of specific threats. The platform also includes a phishing simulator for running phishing simulations on the workforce to reinforce training and identify knowledge gaps. If a phishing simulation is failed, training is automatically delivered to the user in real time, relevant to the threat they failed to identify. This ensures training is delivered at the point when it is likely to be most effective.

For more information on TitanHQ solutions, including the WebTitan DNS filter and the SafeTitan security awareness training platform, give the TitanHQ team a call today. Both solutions are available on a free trial to allow you to assess them fully before making a purchase decision.

Cracked Software Used to Deliver Information Stealing Malware

by G Hunt | February 20, 2025 | Phishing & Email Spam

Information stealers are one of the most common ways that initial access is gained to business networks, and the extent to which these malware variants are used is alarming. According to Hudson Rock, an estimated 30 million computers have been compromised using information stealers in the past few years and Check Point reports that infections have increased by 58% in the past year.

Cybercriminals specialized in infecting devices distribute their information stealers, which collect sensitive data such as session cookies and login credentials, allowing access to be gained to corporate networks. Oftentimes, the cybercriminals then sell that access to other cybercriminal groups, acting as initial access brokers. The groups that they work with have their own specialisms, such as conducting ransomware attacks. These malware variants are capable of stealing large amounts of sensitive information from compromised devices. They can exfiltrate files, obtain web browser data and passwords, and steal cryptocurrency extensions. Infection with an information stealer

can result in the large-scale theft of data, compromised accounts, and further attacks, including ransomware infections.

Security researchers have recently uncovered a new campaign that distributes information stealers such as Lumma and ACR Stealer via cracked versions of legitimate software. The pirated software can be obtained and used free of charge, albeit illegally, and is available through warez sites and from peer-to-peer file-sharing networks. The installers have been packaged to silently deliver an information stealer. Cybercriminals often use SEO poisoning to get their malicious sites to appear high in search engine listings or add malicious adverts to legitimate ad networks (malvertising) to get them to appear on high-traffic websites. The adverts direct internet users to download sites. Initial contact is also made via email, with workers tricked into opening malicious files that launch scripts that deliver the information stealer payload or direct users to websites where the malware is downloaded under the guise of a legitimate program. Contact may also be made via the telephone, with the criminals impersonating IT helpdesk staff and tricking employees into downloading the malware.

Defending against information stealers means improving defenses against all these tactics, and that means there is no single cybersecurity solution or measure that will be effective against them all, but there are three important cybersecurity measures that you should strongly consider: anti-spam software, a DNS filter, and security awareness training.

Anti-spam Software

Many malware infections occur via email, either through attachments containing malicious scripts or via hyperlinks to websites from which malware is downloaded. When malicious attachments are used, they are not always detected by antispam software and can easily reach end users. To improve detection, email sandboxing is required, where messages are sent to the sandbox for deep inspection. In the sandbox, hyperlinks are also followed to identify any downloads that are triggered. If malicious actions are confirmed, the messages are quarantined and are not deleted.

A DNS Filter

Since many malware infections occur via the Internet, businesses should consider web filtering software. DNS-based web filters allow businesses to control the web content that users can access, block certain file downloads from the internet, and assess web content in real-time for malicious content, without the latency associated with other types of web filters. A DNS filter can prevent users from accessing malicious content and will reduce reliance on employees recognizing and avoiding threats.

Security Awareness Training

Anti-spam software and DNS filters will greatly improve security; however, employee security awareness also needs to be improved. Through regular security awareness training, businesses can eliminate risky practices and train employees how to recognize and avoid threats. By providing training continuously in small chunks throughout the year, businesses can develop a security culture and significantly improve their human defenses.

TitanHQ offers multi-award-winning cybersecurity solutions for SMBs and managed service providers (MSPs) that are easy to implement and offer exceptional protection, including the SpamTitan cloud-based spam filtering service, the WebTitan DNS filter, and the SafeTitan security awareness training and phishing simulation solution. All three solutions are available on a free trial to allow you to see for yourself the difference they make before making a purchase decision. Give the TitanHQ team a call to find out more and to discuss these options, and take the important first step toward improving your defenses.

New Phishing Kit Bypasses MFA in Real-Time

by G Hunt | February 18, 2025 | Phishing & Email Spam

A growing number of businesses are implementing multi-factor authentication to add an extra layer of security and improve defenses against phishing attacks. While multifactor authentication (MFA) can prevent unauthorized individuals from accessing accounts using compromised credentials, MFA does not provide total protection. Several phishing kits are sold on hacking forums and Telegram that are capable of bypassing MFA, and a new phishing kit has recently been identified that can intercept credentials in real-time and bypass MFA through session hijacking. The phishing kit is being used to steal credentials and access Gmail, Yahoo, AOL, and Microsoft 365 accounts.

The Astaroth phishing kit has been offered on cybercrime forums since at least January 2025. Similar to the Evilginx phishing kit, Astaroth uses a reverse proxy to intercept and manipulate traffic between the victim and the legitimate authentication of the account being targeted. A cybercriminal can use the Astaroth phishing kit in an adversary-in-the-middle attack, capturing not only login credentials but also 2FA tokens and session cookies, thereby bypassing MFA. The credential theft and session hijacking take place in real time, allowing the cybercriminal to instantly access the user’s account.

The user is presented with a phishing link, which is commonly communicated via email. If that link is clicked, the user is directed to a server and is presented with what appears to be a legitimate login page. The page has valid SSL certificates, so no security warnings are generated. The server acts as a reverse proxy, and when the username and password are entered, they are captured and forwarded to the legitimate authentication service in real time.

The cybercriminal is alerted about the credential capture via the admin panel of the phishing kit or via Telegram, and the one-time passcodes, usually generated via SMS, push notifications, or authentication apps, are intercepted as they are entered by the user. When session cookies are generated, they are immediately hijacked and injected into the attacker’s browser, which means the attacker can impersonate the genuine user without needing their username, password, or 2FA token, since the session has already been authenticated. The kit also includes bulletproof hosting and reCAPTCHA bypasses and allows the attacker to access the account immediately before the user suspects anything untoward has happened.

Phishing kits such as Astaroth are able to render multifactor authentication useless, demonstrating why it is so important to have effective anti-spam software, capable of identifying and blocking the initial phishing emails. SpamTitan is frequently rated as the best spam filter for business due to its ease of implementation and use, exceptional detection, and low false positive rate. TitanHQ also offers MSP spam filtering, with the solution developed from the ground up to meet all MSP needs. In recent independent tests by VirusBulletin, SpamTitan

outperformed all other tested email security solutions, achieving the highest overall score thanks to a 100% malware catch rate, 100% phishing catch rate, 99.999% spam catch rate, and a 0.000% false positive rate. The exceptional performance is due to extensive threat intelligence feeds, machine learning to identify phishing attempts, and email sandboxing to detect and block malware and zero-day threats.

In addition to an advanced spam filtering service, businesses should ensure they provide regular security awareness training to the workforce and reinforce training with phishing simulations. SafeTitan from TitanHQ is an easy-to-use security awareness training platform that makes it easy to create effective training courses and automate the delivery of training content. The platform also includes a phishing simulator with an extensive library of phishing templates that makes it easy to create and automate phishing simulations, generating relevant training automatically if a user is tricked. That means training is delivered at the point when it is likely to be most effective at correcting behavior.

Give the TitanHQ team a call today for more information about these solutions. TitanHQ's SpamTitan and SafeTitan products, like all TitanHQ solutions, are also available on a free trial.

Phishing Campaign Targets European and American Corporate Facebook Accounts

by G Hunt | February 16, 2025 | Security Awareness, Spam Software

A phishing campaign has been identified that targets corporate Facebook credentials and has so far involved more than 12,000 messages to users worldwide. The campaign has primarily targeted enterprises in the European Union (45.5%), United States (45%), and Australia (9.5%) with the phishing emails sent using a legitimate Salesforce automated mailing service. When emails are sent via this service, a sender email address can be specified; however, if no address is supplied, the emails appear to have been sent directly from Salesforce from the noreply@salesforce.com email address, per the terms of service. As such, any recipient of the email may mistakenly believe that the emails are official.

The emails include fake versions of the Facebook logo, which recipients should be able to identify as fake; however, the emails are well-written, and the subject matter is sufficiently concerning to warrant a click. The emails warn the recipient about a copyright infringement claim that has been filed under the Digital Millennium Copyright Act (DMCA) against the user's personal account, indicating material has been shared via their account that is in violation of copyright laws.

The messages include the date of the complaint, that it was reported by Universal Music Group, and is due to the unauthorized use of copyrighted music. The recipient is told they must respond to the claim by the close of business if they wish to contest the claim. The date of the required response is only 24 hours after the complaint date, therefore an immediate response is required. As is common with phishing attempts, there is a threat – permanent restrictions on the user's Facebook account. The message includes a button to click to contest the claim, but rather than direct the user to a login page, they are directed to a fake support page, where they are provided with further information on the restrictions that have or will be applied. Several variations of that email have been identified, including warnings that Facebook surveillance systems have identified a copyright issue and, as a result, limitations have been placed on the user's account.

Those restrictions include the disabling of personal ad accounts and audiences, blocking the management of advertising assets or people for businesses, and preventing the user from creating or running ads and managing ad accounts. In order to have those restrictions removed, the user must click the button to request a review, which directs the user to a spoofed Facebook login page. If credentials are entered, they will be captured and used to log in to the user's account. The campaign, identified by Check Point Research, targets business users, many of whom will rely on Facebook for advertising and customer contact, therefore the consequences of an account restriction could be serious, and certainly serious enough to warrant filing an appeal. What is unclear is how the threat actor uses the compromised accounts. Potentially they could be used for further scams, which could cause considerable reputational damage to the business.

Protecting against these types of phishing campaigns requires a combination of email security and user awareness. An email security solution can prevent these messages from reaching inboxes, thus neutralizing the threat, but security awareness training should also be provided to workforce members to help them identify and avoid phishing attempts. In this case, Facebook admins for the business should be warned about the campaign and instructed to log in to Facebook directly via their web browser if they receive any copyright infringement notices purporting to have been sent by Facebook. If there is a problem with their account, it will be apparent when login into their account.

With the SafeTitan security awareness training platform from TitanHQ, it is easy to create and automate security awareness training programs and roll out new training content in relation to specific threats, only providing that training to the individuals who are likely to be targeted. Phishing simulations can easily be created to test awareness of these phishing scams, with relevant training automatically delivered in response to clicks on phishing emails.

TitanHQ's anti-spam software, SpamTitan, provides excellent protection against phishing, as demonstrated by recent tests by VirusBulletin. The cloud-based anti-spam service outperformed all other antispam solutions in the latest round of tests, blocking 100% of phishing emails and 100% of malware, earning SpamTitan the top spot for overall score. If you are not happy with your anti-phishing defenses or feel you are paying too much for protection, give the TitanHQ team a call and ask about SpamTitan. If you have yet to provide regular security awareness training to your workforce, why not sign up for a free trial of Safetitan and put the product to the test on your workforce?

Email Bombing: What You Need to Know to Protect Your Business

by G Hunt | February 3, 2025 | Phishing & Email Spam, Security Awareness, Spam Software

Investigations of cyberattacks have identified an increasing number of incidents that started with email bombing. A high percentage of cyberattacks involve phishing, where emails are sent to employees to trick them into visiting a malicious website and disclosing their credentials, or opening a malicious file that installs malware. Email bombing is now being used to increase the effectiveness of phishing campaigns.

With email bombing, the user is sent a large number of spam emails in a short period of time, such as by adding a user to a large number of mailshots, news services, and spam lists. The threat actor creates a genuine spam issue then impersonates a member of the IT department and claims they can fix the problem, with content often made

via a Microsoft Teams message. If the user accepts, they are tricked into installing remote access software and granting the threat actor remote access to their device. The threat actor will establish persistent access to the user's device during the remote access session. What starts with an email bombing attack often ends with a ransomware attack.

There are several measures that you should consider implementing to prevent these attacks. If you use Microsoft Teams, consider restricting calls and messages from external organizations, unless there is a legitimate need to accept such requests. If so, ensure permission is only given to trusted individuals such as business partners. The use of remote access tools should be restricted to authorized personnel only, and steps should be taken to prevent the installation of these tools, including using a web filter to block downloads of these tools (and other executables) from the Internet.

An spam filter should be implemented to block spam and unwanted messages. Advanced spam filters such as SpamTitan use AI-guided detection and machine learning to block spam, phishing, and other malicious emails, along with email sandboxing to identify novel threats and zero-day malware. In the Q4, 2024, tests at VirusBulletin, the SpamTitan spam filtering service blocked 99.999% of spam emails, 100% of phishing emails, and 100% of malware with a 0.000% false positive rate, earning SpamTitan top position out of all anti-spam software under test.

Businesses should not underestimate the importance of security awareness training and phishing simulations. Regular security awareness training should be provided to all members of the workforce to raise awareness of the tactics used by cybercriminals. A cyberattack is much more likely to occur as a result of a phishing or social engineering attempt than the exploitation of a software vulnerability. Businesses that use the SafeTitan security awareness training platform and phishing simulator have reduced susceptibility to email attacks by up to 80%. For more information on TitanHQ cybersecurity solutions, including award-winning anti-spam solutions for managed service providers, give the TitanHQ team a call or take advantage of a free trial of any of TitanHQ's cybersecurity solutions.

Microsoft 365 Accounts Targeted Using Sneaky 2FA Phishing Kit

by G Hunt | January 31, 2025 | Phishing & Email Spam, Security Awareness, Spam News

As the massive cyberattack on Change Healthcare demonstrated last year, the failure to implement multifactor authentication on accounts can be costly. In that attack, multifactor authentication was not implemented on a Citrix server, and stolen credentials allowed access that resulted in the theft of the personal and health information of 190 million individuals. The ransomware attack caused a prolonged outage and remediation and recovery cost Change Healthcare an estimated $2.9 billion last year.

The attack should serve as a warning for all companies that multifactor authentication is an essential cybersecurity measure – If passwords are compromised, access to accounts can be prevented. Unfortunately, multifactor authentication protection can be circumvented. Threat actors are increasingly using phishing kits capable of intercepting multifactor authentication codes in an adversary-in-the-middle attack. Phishing kits are packages offered to cybercriminals that cover all aspects of phishing. If purchased, phishing campaigns can be conducted with minimal effort as the phishing kit will generate copies of websites that impersonate well-known brands, the

infrastructure for capturing credentials, and templates for phishing emails. After paying a fee, all that is required is to supply the email addresses for the campaign, which can be easily purchased on hacking forums.

Some of the more advanced phishing kits are capable of defeating multifactor authentication by harvesting Microsoft 365 and Gmail session cookies, which are used to circumvent MFA access controls during subsequent authentication. One of the latest phishing kits to be identified is has been dubbed Sneaky 2FA. The kit was first identified as being offered and operated on Telegram in October 2024 by researchers at the French cybersecurity firm Sekoia. The researchers identified almost 100 domains that host phishing pages created by the Sneaky 2FA phishing kit.

As with a standard phishing attack, phishing emails are sent to individuals to trick them into visiting a phishing page. One campaign using the Sneaky 2FA phishing kit uses payment receipt-related emails to trick the recipient into opening a PDF file attachment that has a QR code directing the user to a Sneaky 2FA page on a compromised website, usually a compromised WordPress site. These pages have a blurred background and a login prompt. Microsoft 365 credentials are required to access the blurred content. The phishing pages automatically add the user's email address to the login prompt, so they are only required to enter their password. To evade detection, multiple measures are employed such as traffic filtering, Cloudfire Turnstile challenges, and CAPTCHA checks.

Many phishing kits use reverse proxies for handling requests; however, the Sneaky 2FA phishing server handles communications with Microsoft 365 API directly. If the checks are passed, JavaScript code is used to handle the authentication steps. When the password is entered, the user is directed to the next page, and the victim's email address and password are sent to the phishing server via an HTTP Post. The server responds with the 2FA method for the victim's account and the response is sent to the phishing server. The phishing kit allows session cookies to be harvested that provide account access, regardless of the 2FA method – Microsoft Authenticator, one-time password code, or SMS verification.

Phishing kits such as Sneaky FA make it easy for cybercriminals to conduct phishing attacks and defeat MFA; however, they are not effective at defeating phishing-resistant MFA such as FIDO2, WebAuthn, or biometric authentication. The problem is that these forms of MFA can be expensive and difficult to deploy at scale.

Businesses can greatly improve their defenses with advanced spam filter software with AI- and machine learning detection, email sandboxing, URL rewriting, QR code checks, greylisting, SPF, DKIM, and DMARC checks, and banners identifying emails from external sources. Effective email filtering will ensure that these malicious emails do not land in employee inboxes. TitanHQ offers two email security solutions – SpamTitan email security and the PhishTitan anti-phishing solution for M365. The engine that powers both solutions was recently rated in 1st place for protection in the Q4, 2024 tests by VirusBulletin, achieving a 100% malware and 100% phishing detection rate.

Regular security awareness training should also be provided to all members of the workforce to raise awareness of threats and to teach cybersecurity best practices. With the SafeTitan security awareness training platform it is easy to create and automate training courses and add in new training content when new threat actor tactics are identified. The platform also includes a phishing simulator for reinforcing training and identifying individuals in need of additional training.

For more information on improving your defenses against phishing and malware, give the TitanHQ team a call. Product demonstrations can be arranged on request and all TitanHQ solutions are available on a free trial.

AI-Generated Voice Phishing Calls Combined with Email to Steal Gmail Credentials

by G Hunt | January 26, 2025 | Phishing & Email Spam

Cybercriminals often devise phishing lures that can be used on as many individuals as possible, which is why they often impersonate big-name brands such as Microsoft, Apple, Facebook, and Google, since there is a high percentage chance that the emails will land in the inbox of someone that uses the products of those companies.

In the case of Google, a phishing campaign targeting Gmail account holders makes sense from the perspective of a cybercriminal as there are around 2.5 billion Gmail users worldwide. One such campaign has recently been identified that uses a combination of an email and a phone call to obtain account credentials. Email accounts can contain a wealth of sensitive information that can be misused or used in further attacks on an individual, and the accounts can be used for phishing and spear phishing campaigns.

Phishing campaigns that combine multiple communication methods are becoming more common, such as callback phishing. With callback phishing, the scam starts with an email devoid of malicious links, scripts, and attachments. The recipient is told that a charge will be applied to their account for a subscription or free trial that is coming to an end. The user is informed that they must call the number in the email to terminate the subscription before the charge is applied. If the number is called, the threat actor uses social engineering techniques to trick the user into downloading a remote access solution to remove the software and prevent the charge. The software gives the threat actor full control of their device.

The latest campaign uses emails and phone calls in the opposite order, with initial contact made via the phone by a person impersonating the Google support team. The reason for the phone call is to advise the Gmail user that their account has been compromised or suspended due to suspicious activity, or that attempts are being made to recover access.

One user received a call where a Google customer support worker told them that a family member was trying to gain access to their account and had provided a death certificate. The call was to verify the validity of the family member’s claim. People targeted in this campaign may attempt to verify the validity of the call by checking the phone number; however, Caller ID is spoofed to make it appear that the call has come from a legitimate Google customer support number.

The second phase of the scam includes an email sent to the user’s Gmail account corroborating the matter discussed in the phone call, with the email requiring action to recover the account and reset the password. A link is provided that directs the user to a spoofed login page where they are required to enter their credentials, which are captured by the scammer. There have also been reports where initial contact is made via email, with a follow-up telephone call.

Performing such a scam at scale would require a great deal of manpower, and while telephone scams are commonly conducted by call center staff in foreign countries, this scam involves AI-generated calls. The caller

sounds professional and polite and has a native accent, but the victim is not conversing with a real person. The reason for the call is plausible, the voice very realistic, and the scam is capable of fooling even security-conscious individuals.

Businesses looking to improve their defenses against advanced phishing scams should ensure that they cover these types of sophisticated phishing attempts in their security awareness training programs. Employees should be told that threat actors may use a variety of methods for contact, often combining more than one communication method in the same scam. Keeping employees up to date on the latest tactics used by scammers is straightforward with the SafeTitan security awareness training platform. New training content can easily be created in response to changing tactics to keep the workforce up to date on the latest scams. SafeTitan also includes a phishing simulator for reinforcing training.

An advanced email security solution is also strongly recommended for blocking the email-based component of these sophisticated phishing scams. SpamTitan cloud based anti spam software incorporates machine learning capable of identifying previous unseen phishing scams, ensuring phishing attempts are blocked and do not land in inboxes. In recent independent tests at VirusBulletin, SpamTitan achieved the top spot due to comprehensive detection rates, blocking 100% of malware and phishing emails, and 99.999% of spam emails. To block sophisticated AI-generated phishing attempts you need sophisticated AI-based defenses. Give the TitanHQ team a call today to find out more about improving your defenses against AI-based attacks.

AI-Generated Phishing Emails Trick More Than 50% of Recipients

by G Hunt | January 15, 2025 | Phishing & Email Spam

Large language models (LLMs) are used for natural language processing tasks and can generate human-like responses after being trained on vast amounts of data. The most capable LLMs are generative pretrained transformers, or GPTs, the most popular of which is ChatGPT, although there are many others including the China-developed DeepSeek app.

These AI-powered tools have proven incredibly popular and are used for a wide range of tasks, eliminating a great deal of human effort. They are used for creating articles, resumes, job applications, and completing homework, translating from one language to another, creating summaries of text to pull out the key points, and writing and debugging code to name just a few applications.

When these artificial intelligence tools were released for public use, security professionals warned that in addition to the beneficial uses, they could easily be adopted by cybercriminals for malicious purposes such as writing malware code, phishing/spearphishing, and social engineering.

Guardrails were implemented by the developers of these tools to prevent them from being used for malicious purposes, but those controls can be circumvented. Further, LLMs have been made available specifically for use by cybercriminals that lack the restrictions of tools such as ChatGPT and DeepSeek.

Evidence has been growing that cybercriminals are actively using LLMs for malicious purposes, including writing flawless phishing emails in multiple languages. Human-written phishing emails often contain spelling mistakes

and grammatical errors, making them relatively easy for people to identify but AI-generated phishing emails lack these easily identified red flags.

While cybersecurity professionals have predicted that AI-generated phishing emails could potentially be far more effective than human-generated emails, it is unclear how effective these AI-generated messages are at achieving the intended purpose – tricking the recipient into disclosing sensitive data such as login credentials, opening a malicious file, or taking some other action that satisfies the attacker's nefarious aims.

A recently conducted study set out to explore how effective AI-generated spear phishing emails are at tricking humans compared to human-generated phishing attempts. The study confirmed that AI tools have made life much easier for cybercriminals by saving them a huge amount of time. Worryingly, these tools significantly improve click rates.

For the study, researchers from Harvard Kennedy School and Avant Research Group developed an AI-powered tool capable of automating spear phishing campaigns. Their AI agents were based on GPT-4o and Claude 3.5 Sonnet, which were used to crawl the web to identify information on individuals who could be targeted and to generate personalized phishing messages.

The bad news is that they achieved an astonishing 54% click-through rate (CTR) compared to a CTR of 12% for standard phishing emails. In a comparison with phishing emails generated by human phishing experts, a similar CTR was achieved with the human-generated phishing emails; however, the human version cost 30% more than the cost of the AI automation tools.

What made the phishing emails so effective was the level of personalization. Spear phishing is a far more effective strategy than standard phishing, but these attacks take a lot of time and effort. By using AI, the time taken to obtain the personal information needed for the phishing attempt and develop a lure relevant to the targeted individual was massively reduced. In the researchers' campaign, the web was scraped for personal information and the targeted individuals were invited to participate in a project that aligned with their interests. They were then provided with a link to click for further information. In a genuine malicious campaign, the linked site would be used to deliver malware or capture credentials.

AI-generated phishing is a major cause of concern, but there is good news. AI tools can be used for malicious purposes, but they can also be used for defensive purposes and can identify the phishing content that humans struggle to identify. Security professionals should be concerned about AI-generated phishing, but email security solutions such as SpamTitan can give them peace of mind.

SpamTitan, TitanHQ's cloud-based anti-spam service, has AI and machine learning capabilities that can identify human-generated and AI-generated phishing attempts, and email sandboxing for detecting zero-day malware threats. In recent independent tests, SpamTitan outperformed all other email security solutions and achieved a phishing and malware catch rate of 100%, a spam catch rate of 99.999%, with a 0.000% false positive rate. When combined with TitanHQ's security awareness training platform and phishing simulator – SafeTitan, security teams will be able to sleep easily.

For more information about SpamTitan, SafeTitan, and other TitanHQ cybersecurity solutions for businesses and managed service providers, give the TitanHQ team a call. All TitanHQ solutions are available on a free trial and

product demonstrations can be arranged on request.

Remcos RAT Infections of the Rise as Threat Actors Adopt New Phishing Tactics

by G Hunt | December 29, 2024 | Phishing & Email Spam, Spam Software

Detections of the Remcos remote access trojan (RAT) have increased recently with threat actors adopting new tactics to deliver this popular commercially available malware. The Remcos RAT is offered under the malware-as-a-service model, where purchasers can use the malware to remotely control infected devices and steal sensitive data.

The Remcos RAT is primarily delivered via phishing emails with malicious attachments, with each of the two main variants delivered using distinct methods. One of the variants is distributed in phishing emails using Microsoft Office open XML attachments that exploit a Microsoft Office memory corruption remote code execution vulnerability (CVE-2027-11882) to execute an embedded script that downloads an intermediate payload that will in turn deliver the Remcos RAT. The vulnerability does not affect newer Office versions, such as Microsoft 365, only older versions prior to Office 2016.

Lures commonly used include fake purchase orders, where the email claims to include purchasing specifications in the attached Excel file. If opened, the spreadsheet is blurred and the user is told the document is protected, and to enable editing to view the file. In the background, the vulnerability is exploited to deliver and execute an HTA file, triggering the processes that lead to the installation of the Remcos RAT. When delivered, the Remocos RAT is injected into a legitimate Windows executable (RegAsm.exe).

The second variant uses a VBS attachment with an obfuscated PowerShell script to download files from a remote server and inject code into RegAsm.exe. Since the final payload is injected into legitimate Windows processes, the malware is often not detected by security solutions. Once installed, persistence is maintained via registry modifications to ensure the malware remains active after a reboot. Lures used to deliver this variant include payment confirmations, with details included in the attached DOCX file.

The highest number of infections have occurred in the United States and India, and there has been a sharp rise in infections in recent months showing that the campaigns are proving effective. A combination of technical measures and security awareness training will help to prevent Remcos RAT infections. Phishing campaigns such as this show why it is important to stay on top of patching and ensure that all systems are kept up to date, and to migrate from software that has reached end-of-life to supported software versions. Endpoint security software is important; however, detection of the Remcos RAT can be difficult since files are not written to the hard drive.

The primary defense is an advanced email security solution. SpamTitan, TitanHQ's spam filtering service, is an ideal choice as it includes reputation checks, SPF, DKIM, & DMARC, machine-learning algorithms to identify anomalies in emails, and email sandboxing, where attachments are sent for extensive analysis including pattern filtering. In recent tests by VirusBulletin, the engine that powers SpamTitan scored highest out of all 11 tested email security solutions, with a 100% malware and phishing catch rate.

It is important to keep the workforce up to date on the latest security threats and to teach and reinforce security best practices. The SafeTitan security awareness training platform makes this easy for businesses and MSPs,

allowing effective security awareness training programs to be created that are tailored to individuals and user roles. The training can be automated to be delivered regularly to employees, as can phishing simulations using the SafeTitan phishing simulator to test the effectiveness of training. Businesses with Microsoft 365 would benefit from the PhishTitan platform. Based on the same engine that powers SpamTitan, PhishTitan helps to protect Microsoft 365 environments from the advanced threats that Microsoft fails to block, add banners to emails from external sources and helps security teams rapidly mitigate phishing threats.

Google Calendar Abused in Phishing Campaign

by G Hunt | December 28, 2024 | Phishing & Email Spam

Companies in multiple sectors are being targeted in an ongoing phishing campaign involving initial contact via email via Google Calendar-generated meeting invites. This campaign has proven effective, especially when the user recognizes other guests. The campaign has been active throughout December, with at least 1,000 of these phishing emails identified each week, according to Check Point.

The aim of the phishing emails is to trick the recipients into clicking a link in the email or opening a Calendar file attachment (.ics), both of which will send the user to either Google Forms or Google Drawings. Next, the user is tricked into clicking another link, which could be a support button or a fake reCAPTCHA. A click will drive the user to the scam page, where they will be taken through a fake authentication process that captures personal information, and ultimately payment card information. This campaign could easily be adapted to obtain credentials rather than payment card details, and campaigns in the past that abused Google Calendar have targeted credentials.

An attacker only needs to obtain an individual's email address to send the calendar invite, and the emails look exactly like a genuine invite for a meeting. Since the legitimate Google Calendar service is used to generate the phishing invites, the emails are generally not blocked by spam filtering services. Since the sender is legitimate and trusted, the emails pass SPF, DKIM, and DMARC checks, guaranteeing delivery.

Depending on the user's settings, these may be automatically added to the user's calendar. The threat actor can then trigger a second email by canceling the meeting and has been doing so in this campaign. The cancellation email also includes a hyperlink to a malicious website.

The use of Google Calendar invites in phishing is nothing new. It is effective as it ensures a large number of requests land in inboxes, and Google Calendar will be familiar to most people, considering there are more than 500 million active users of the tool.

There are simple steps to take to block these threats, although the first option will also limit legitimate functionality for genuine invites. To block these attempts, go into Google Calander settings, and in the event settings switch from automatically add invitations to only show invitations I have responded to. Also, access Gmail settings and uncheck automatically add events from Gmail to my calendar. To avoid disabling the functionality, check the only known individuals setting in Google Calendar, which will generate an alert if the user has had no interactions with an individual in the past.

It is important to have an advanced email security solution that is capable of detecting sophisticated phishing attacks that bypass the standard reputation checks that are present in virtually all spam filtering software – SPF, DKIM, and DMARC. Advanced spam filtering solutions incorporate AI and machine learning capabilities and can detect anomalies in inbound emails and flag them as suspicious or send them for deeper inspection in an email sandbox. In the sandbox, the message can be analyzed for malicious content, including following the link to check the destination URL. While this campaign does not use malware, an email filtering service with email sandboxing will also protect against malware threats.

Meeting invites, calendar invites, and collaboration requests are commonly used in phishing campaigns and are sent from trusted domains that often bypass spam filtering controls, so it is important to cover these types of scam emails in security awareness training. Employees should be made aware that these requests may not be what they seem, even if they have been sent via a legitimate service. Businesses can also gauge how susceptible employees are to these types of scams using a phishing simulator. SafeTitan includes many phishing templates involving invites from legitimate services to allow businesses to incorporate these into their simulations.

Call TitanHQ today for more information on improving your defenses against phishing with the SafeTitan security awareness training platform, SpamTitan email security, and the PhishTitan anti-phishing solution for Microsoft 365.

TitanHQ Achieves 1st Place in Q4 Virus Bulletin Email Security Tests

by G Hunt | December 23, 2024 | Industry News, Spam Software

TitanHQ's email security solutions achieved first place in Q4 performance tests by the leading security information portal, testing, and certification body, VirusBulletin. The security engine that powers TitanHQ's SpamTitan email security and PhishTitan anti-phishing platform for Microsoft 365 was put to the test alongside 10 other market-leading email security solutions and achieved the highest overall score out of all 11 solutions, building on the joint 1st overall score in the Q3, 2024 round of tests, 2nd position in the Q3 tests, and 3rd position in the Q1, 2024 tests.

The top position was achieved with a 100% phishing catch rate, a 100% malware catch rate, and a 0.00% false positive rate. This was the third consecutive quarter that TitanHQ's solutions had a perfect score for catching malware and the third consecutive quarter that TitanHQ has been awarded the VBSpam+ award for outstanding performance. "We are thrilled to have significantly outperformed our main competitors and surpassed the industry average," said TitanHQ CEO, Ronan Kavanagh. "Our unwavering commitment to providing unmatched email security is evident in these results, and we remain dedicated to protecting our clients from evolving cyber threats."

Over the past two decades, VirusBulletin has tested, reviewed, and benchmarked enterprise-level security solutions to determine how effective the solutions are at blocking real-world threats. VirusBulletin has a formidable reputation for providing businesses with invaluable independent intelligence about the rapidly evolving threat landscape, and businesses look to performance tests when selecting security solutions to make sure they perform as well as the vendors' claim. For the Q4, 2024 tests of enterprise-level anti-spam software, TitanHQ's cloud-based anti-spam service was put to the test alongside solutions from Bitdefender, Fortinet, Mimecast, N-able, Sophos, Rspamd, SEPPmail, Net at Work, and Zoho. The tests ran for 16 days in November

2024 and included evaluations of almost 107,000 emails, of which 105,228 were spam and 1,315 were legitimate emails. 1,045 of the emails contained a malicious attachment and 16,825 contained a link to a web page hosting phishing content or malware.

Virus Bulletin Q4, 2024 Test Scores

Metric	TitanHQ Score
Malware catch rate	100.000%
Phishing catch rate	100.000%
Spam Catch (SC) rate	99.999%
Project Honey Pot SC rate	99.998%
MXMailData SC rate	100.000%
Abusix SC rate	99.999%
False Positive (FP) Rate	0.000%
Newsletters FP rate	0.0%
Final Score	**99.999%**

“With only two spam samples missed – one of which was from the unwanted category – no false positives of any kind, and a final score value of 99.999, *SpamTitan* showed the best performance in this test, ranking top for final score,” explained VirusBulletin. “Needless to say, a well-deserved VBSpam+ certification is awarded.”

Virus Bulletin 2024 Test Scores

Test Period	Phishing catch Rate	Malware Catch Rate	Spam Catch Rate	Position
Q1	99.91%	99.95%	99.98%	3rd
Q2	99.99%	100%	99.98%	2nd
Q3	99.98%	100%	99.98%	1st (Joint)
Q4	100%	100%	99.99%	1st

The test results confirm that TitanHQ is a leading enterprise spam filter provider; however. TitanHQ’s spam filtering service and anti-phishing solution for M365 are suitable for use by businesses of all sizes. While incredibly powerful and feature-rich, they are easy to implement and use. The solutions have also been developed from the ground up to meet the needs of MSPs to help them better protect their clients from rapidly evolving threats. “We’ve seen a remarkable influx of new MSP customers migrating from other solutions, consistently highlighting TitanHQ’s ability to deliver immediate and substantial threat mitigation,” said Kavanagh.

If you want industry-leading email protection from spam, phishing, and malware, give the TitanHQ team a call today to find out more about getting started with SpamTitan and PhishTitan. Product demonstrations can be arranged on request and all TitanHQ solutions are available on a free trial.

SpamTitan Enhanced with Latest Skellig 9.07 Release

by G Hunt | December 18, 2024 | Industry News, Spam Software

TitanHQ has announced that the latest version of SpamTitan (Skellig 9.07) has been launched, offering significant enhancements to improve detection, usability, and overall security. The new version of SpamTitan Skellig builds on previous versions that have been demonstrated to provide exceptional protection against malware, phishing, and spam, as evidenced by recent independent tests by VirusBulletin.

In Q3, 2024, SpamTitan achieved joint first place for overall score in the phishing, spam, and malware detection tests, and in Q4, 2024, performed even better beating all other industry-leading competitors to achieve the top spot with an overall score of 99.999%, including a malware and phishing catch rate of 100%, a spam catch rate of 99.999%, and a false positive rate of 0.000%, earning SpamTitan its third consecutive VPSpam+ award.

The latest release of the SpamTitan Skellig engine includes numerous security updates, including significant improvements with enhanced Domain and Display Name anti-spoofing protection and updated anti-spoofing screens. The settings for Domain and Display Name anti-spoofing have been separated to make it easier to see which features have been enabled and the update makes MSP’s lives easier as these split options are available at the customer level, so there is no need to drill down to each domain-level setting. The update will reduce the time that needs to be spent managing security defenses. Further, the update provides greater flexibility and control for inbox protection, since Display Name anti-spoofing is independent of user policies. That means it is possible to upload a custom list of Display Name/email pairs for more targeted protection. To improve usability, changes have also been made under the cover for Quarantine Reports to ensure they are delivered more reliably and on-time

TitanHQ is committed to making continuous security improvements to improve detection and simplify security management to make its products easier and less time-consuming to use, ensuring users have complete control of how protections are applied. The new version will be updated automatically for current users, and if you are yet to try our spam filtering service, give the TitanHQ team today for help getting you started with a free trial.

Threat Actors Adopt Corrupted Word Files for Phishing Campaigns

by G Hunt | December 16, 2024 | Phishing & Email Spam

A new phishing campaign has been identified that uses the novel tactic of attaching corrupted Microsoft Word files to emails. The files themselves do not contain any malicious code, so scans of the attachments by email security solutions may not flag the emails as malicious.

In order to get the recipient to open the email, the threat actor impersonates the HR department or payroll team, as employees will typically open these messages. The attached files have file names related to payments, annual benefits, and bonuses, which employees may open without performing standard checks of the email, such as

identifying the true sender of the message. Many employees place a moderate amount of trust in Word files, as if they contain a macro, it should not run automatically if the Word document is opened.

The threat actor relies on the employee's curiosity to open the file and the way that operating systems handle corrupted files. The file recovery feature of Microsoft Word will attempt to recover corrupted files. The user will be informed that parts of the file contain unreadable content, and the user is prompted to confirm if they would like the file to be recovered. The documents have been crafted to ensure that they can be recovered by Word, and the recovery will present the user with a QR code that they are told they must scan to retrieve the document.

The document includes the logo of the company being targeted, and the user does not need to "enable editing" to view the contents of the document, so they may mistakenly believe they are safe. If they scan the QR code using their mobile device, they will be directed to a phishing page where they are asked to enter their Microsoft credentials on a phishing page that is an exact match of the genuine Microsoft login prompt.

Businesses with spam filter software may not be protected as email security solutions often fail to scan corrupted files. For instance, the phishing emails bypass Outlook spam filters according to the researchers at Any.Run who identified the campaign. That means the emails may be delivered to inboxes, especially as the messages do not contain any content in the body of the email indicative of a phishing attempt.

If the user opens the file and scans the QR code, they will switch from their desktop or laptop to their mobile phone. Mobile devices rarely have the same level of security protection, so corporate anti-phishing controls such as web filters will likely be bypassed.

Threat actors are constantly developing new ways to trick employees in their phishing campaigns, which is why it is important to run security awareness training programs continuously, updating the training content with new training material in response to threat actors' changing tactics. By warning employees about this method, they should recognize the scam for what it is if they receive an email with a corrupted file attachment. That is easy to do with a security awareness training platform such as SafeTitan. New training content can be quickly created and rolled out to all users as part of their monthly allocation of training modules. It is also easy to add this type of threat to the SafeTitan phishing simulator to test how employees respond to this new threat type.

As the researchers demonstrated, Microsoft fails to detect the threat, demonstrating why it is important to bolster your M365 phishing defenses with a third-party solution, such as PhishTitan from TitanHQ. PhishTitan integrates seamlessly with Microsoft 365 to augment protection and catches the phishing threats that Microsoft misses. PhishTitan will also add a banner to all inbound emails that come from external sources, giving users a clear flag that these emails are not genuine. The HR department and payroll have internal email addresses.

An email security solution with email sandboxing is also advisable for deep inspection of file attachments, including the ability to read QR codes. Spam filters for incoming mail should also have machine learning and AI-based detection capabilities for identifying emails that deviate from the messages typically received by the business.

All of these features are part of TitanHQ's email security suite. Give the team a call today to find out more.

Email Bombing Adopted by Ransomware Groups for Initial Access

by G Hunt | December 12, 2024 | Network Security, Security Awareness

In this post, we explore some of the tactics used by the Black Basta ransomware group to gain initial access to victims' networks. Black Basta is a ransomware-as-a-service (RaaS) group that first appeared in April 2022. After gaining access to victims' networks, the group escalates privileges and moves laterally within the network, identifying sensitive data and exfiltrating files before running its encryption processes. The group then drops a ransomware note and demands payment to prevent the publication of the stolen data and to obtain the keys to decrypt the encrypted files. The group targets multiple industry sectors including healthcare organizations, primarily in North America, Europe, and Australia.

The group's tactics are constantly evolving; however, one of the most common tactics used for initial access is email phishing, either by sending an email with a hyperlink to a malicious website or an infected email attachment. The group's phishing campaigns aim to deliver Qakbot malware, which is used to provide persistent access to victims' networks (via autorun entries and scheduled tasks), and for running PowerShell scripts to disable security solutions. The malware is then used to deliver additional malicious payloads such as Cobalt Strike, and legitimate software tools such as Splashtop, Mimikatz, and Screen Connect.

Recently, the group has been observed using a new tactic called email bombing as an alternative way of gaining initial access to networks. With email bombing, the selected targets' email addresses are sent large volumes of spam emails, often by signing the user up to multiple mailing lists or spamming services simultaneously. After receiving a large volume of spam emails, the user is prepared for the next stage of the attack.

The threat actor reaches out to the user, often via Microsoft Teams or over the phone, and impersonates a member of the IT help desk. The threat actor claims they have identified a problem with spam email and tells the user that they need to download a remote management tool to resolve the issue.

If the user agrees, they are talked through downloading one of several tools such as QuickAssist, AnyDesk, TeamViewer, or ScreenConnect. The threat actor then uses that tool to remotely access the user's device. These tools may be downloaded directly from the legitimate vendor's domain; however, since many businesses have controls in place to prevent the installation of unauthorized remote access tools, the installation executable file may be downloaded from SharePoint. Once installed, the threat actor will use the remote access to deliver a range of payloads.

Email bombing is a highly effective tactic as it creates a need to have an issue resolved. Once on the phone or in conversation via Microsoft Teams, the threat actor is able to try other methods for installing the remote access tools if they fail due to the user's security settings.

Email bombing may be used by multiple threat actors for initial access, and phishing remains the most common method for gaining a foothold in networks for follow-on attacks. Implementing defenses against these tactics will significantly improve your defenses and make it harder for threat actors to breach your network.

An Advanced Spam Filter

An advanced spam filter is a must, as it can identify and block phishing attempts and reduce the effectiveness of email bombing. Next-gen spam filtering software incorporates AI and machine learning algorithms to thoroughly

assess inbound emails, checking how they deviate from the emails typically received by the business, and helping to flag anomalies that could indicate novel phishing attempts.

A spam filter should also incorporate email sandboxing in addition to antivirus software protection, as the latter can only detect known threats. Novel malware variants and obfuscated malware are often missed by antivirus software, so a sandbox is key to blocking malware threats. After passing initial checks, an email is sent to the email sandboxing service for deep analysis, where behavior is checked for malicious actions, such as attempted C2 communications and malware downloads.

SpamTitan incorporates machine learning algorithms, sandboxing, and link scanning to provide advanced protection against phishing and malware attacks. SpamTitan was recently rated the most effective spam filter in recent independent tests by VirusBulletin, blocking 100% of phishing emails, 100% of malware, and 99.99% of spam emails, giving the solution the highest overall score out of all 11 spam filtering services put to the test.

Security Awareness Training

It is important to provide regular security awareness training to the workforce, including all employees and the C-suite. The most effective training is provided regularly in small chunks, building up knowledge of threats and reinforcing security best practices. This is easiest with a modular computer-based training course. When new tactics such as email bombing are identified, they can be easily incorporated into the training course and rolled out to end users to improve awareness of specific tactics. Also consider running phishing simulations, as these have been shown to be highly effective at reinforcing training and identifying knowledge gaps that can be addressed through further training.

TitanHQ makes this as easy as possible with the SafeTitan security awareness training and phishing simulation platform. The platform includes hundreds of engaging and enjoyable training modules covering all aspects of security and threats employees need to be aware of, while the phishing simulation platform makes it easy to create and automate internal phishing simulations, which automatically trigger relevant training content if the user fails the simulation.

Give the TitanHQ team a call today for further information on SpamTitan and Safetitan, for a product demonstration, or to arrange a free trial.

Protect Your Business Against Holiday Season Cyber Threats

by G Hunt | November 30, 2024 | Internet Security, Phishing & Email Spam

Holiday season officially started the day after Thanksgiving in the United States, or Black Friday as it is now known. Taking its name from a term used by police officers in Philadelphia to describe the chaos in the city caused by the deluge of suburban shoppers heading to the city to do their holiday shopping, it has become a day when retailers offer bargains to entice the public to buy their goods and services. While the jury is still out on how good many of those bargains are, the consensus is that there are bargains to be found in stores and online, with the official day for the latter being the Monday after Black Friday – Cyber Monday.

The holiday season for shoppers is boom time for cybercriminals who take advantage of the increase in online shoppers looking to buy gifts for Christmas and pick up a bargain of two. Many people time major purchases to take advantage of Black Friday and Cyber Monday offers and cybercriminals are poised to pounce on the unwary. The losses to scams over the holiday period are staggering. According to the Federal Bureau of Investigation (FBI), more than $73 million was lost to holiday season scams in 2022; however, the true total is likely to be considerably higher since many losses go unreported. Those figures do not include the losses to phishing, malware, ransomware, BEC attacks, and other cyberattacks that occur over the holiday period. For instance, the surge in ransomware attacks over Thanksgiving weekend and Christmas when the IT staff is spread thin.

Given the heightened risk of scams and cyberattacks over the holiday season, consumers should be on their guard and take extra care online and ensure that vendors are legitimate before handing over their card details and double-checking the legitimacy of any email requests. While consumers face elevated risks during the holiday season, so do businesses. There are end-of-year deadlines to meet and it's a short month with many workers taking annual leave over Christmas and the New Year. As the year draws to a close it is common for vigilance to slip, and threat actors are ready to take advantage. Businesses need to ensure that their defenses are up to scratch, especially against phishing – the most common initial access vector in cyberattacks – as a slip in vigilance can easily lead to a costly cyberattack.

Businesses can take several proactive steps to ensure they are protected against holiday season cyber threats, and conducting a security awareness training session is a good place to start. Employees should be reminded about the increase in malicious cyber activity over the holiday period and be reminded about the risks they may encounter online, via email, SMS, instant messaging services, and the phone. With TitanHQ's SafeTitan security awareness training platform, it is easy to spin up training courses for employees to remind them to be vigilant and warn them about seasonal and other cyber threats. The training platform makes it quick and easy to create and automate training courses, with the training delivered in modules of no more than 10 minutes to ensure employees can maintain concentration and fit the training into their workflows. The SafeTitan platform also incorporates a phishing simulator, which businesses can use to reinforce training and identify individuals who are fooled by phishing scams and ensure they receive the additional training they need.

Due to the high risk of phishing attacks, it is a good idea to implement an advanced spam filter service, one that reliably identifies and neutralizes phishing and business email compromise attempts and provides cutting-edge protection against malware. You need look no further than SpamTitan for that protection. SpamTitan incorporates machine learning and AI-based detection capabilities for detecting phishing, BEC, and scam emails, and dual antivirus engines and email sandboxing for detecting malware threats, including novel malware variants. In Q3, VirusBulletin's tests of SpamTitan confirmed a phishing detection rate of 99.99% and a malware catch rate of 99.511%. The interim figures for November 2024 are a 100% phishing catch rate and a 100% malware catch rate, demonstrating the reliability of TitanHQ's cloud-based email filtering solution.

TitanHQ also offers online protection through the WebTitan DNS filter, which prevents access to known malicious websites, blocks malware downloads from the Internet, and can be used to control the web content employees can access, providing an important extra layer of security against web-based threats. At TitanHQ we hope you have a happy holiday period and above all else that you are well protected against cyber threats. Give the team a call today to find out more about how we can help protect your business this holiday season and beyond.

Phishing Campaign Targets Law Firms by Impersonating U.S. Federal Courts

by G Hunt | November 30, 2024 | Phishing & Email Spam

A phishing campaign has been identified that targets law firms by impersonating U.S. federal courts and purports to contain an electronic notice of court filings. Like many similar campaigns in recent months, the campaign aims to trick law firm employees into downloading malware that provides the threat actor with persistent access to the law firm's network.

Threat actors often target businesses, but a far more effective use of their time and resources is to target vendors. If a threat actor gains access to a vendor's network, they can potentially use the vendor's privileged access to attack all downstream clients. Even when a vendor does not have privileged access to client networks, they are likely to store large amounts of data from multiple clients. In the case of law firms, that data is highly sensitive and easily monetized. It can be easily sold on darknet marketplaces and be used as leverage to extort the law firm and its clients.

Over the last few years, law firms have been extensively targeted by threat actors for this very reason. According to a 2023 report from the UK's National Cyber Security Centre, 65% of law firms have been a victim of a cyber incident and a 2024 report from the chartered accountancy firm Lubbock Fine indicates cyberattacks on law firms have increased by 77% year-over-year. The main motivation for these attacks is extortion and ransomware attacks. There has also been a surge in business email compromise (BEC) attacks on law firms, as they are typically involved in large financial transactions that threat actors can try to divert to their own accounts.

One of the latest campaigns seeks persistent access to the networks of law firms by tricking the firms into installing malware. The campaign came to light following multiple complaints about fake notices of electronic court filings, which prompted the U.S. federal judiciary to issue a warning to U.S. lawyers to be alert to email notifications that purport to be notifications from the courts. The emails impersonate the PACER case management and electronic case files system, and instruct the recipient to respond immediately. The judiciary advised law firms to always check the federal judiciary's official electronic filing system and never open attachments in emails or download files from unofficial sources.

The intercepted emails impersonate lower courts and prompt the recipient to click an embedded hyperlink to access a document from a cloud-based repository. Clicking the link directs the user to a malicious website where they are prompted to download a file. Opening the file triggers the installation of malware that will give the threat actor the access they need for an extensive compromise. The campaign will undoubtedly result in the theft of sensitive data and attempted extortion.

Most law firms will be well aware that they are prime targets for threat actors and the importance of implementing robust cybersecurity defenses. Since phishing is the most common way that threat actors get access to their networks and sensitive data, it is vital for law firms to ensure that they have an effective email security solution – one that is capable of detecting and blocking malware and correctly classifying phishing and BEC emails. This is an area where TitanHQ can help. TitanHQ offers a suite of cutting-edge cybersecurity solutions that provide multiple layers of protection against the most common attack vectors.

The primary defense against phishing and BEC attacks is anti-spam software, which TitanHQ can provide as a cloud-based anti-spam service or virtual anti-spam appliance that can be installed on-premises on existing hardware. The SpamTitan solution incorporates dual anti-virus engines and email sandboxing for detecting malware and malicious code in email attachments, even zero-day malware threats. The solution has machine learning capabilities for detecting novel email threats such as phishing and BEC attacks that are needed to detect and block the latest AI-generated threats. In independent tests by Virus Bulletin in November 2024 on 125,000 emails, SpamTitan had a 100% malware and phishing catch rate and only miscategorized 2 benign spam emails.

It is also important to ensure that all lawyers and support staff are made aware of the latest threats and receive regular cybersecurity awareness training. TitanHQ offers a comprehensive security awareness training platform (SafeTitan) and phishing simulator that makes it easy to create effective, ongoing training programs that incorporate training material on the latest threats. Give the TitanHQ team a call today for more information on these and other cybersecurity solutions and for advice on improving your cybersecurity defenses against the most common attack vectors.

SVG Image Files Being Used for Phishing and Malware Delivery

by G Hunt | November 29, 2024 | Phishing & Email Spam

Cybercriminals are increasingly leveraging SVG files in their email campaigns. These file attachments have been used as part of convincing campaigns that have fooled many end users into disclosing their credentials or installing malware.

SVG files, or Scalable Vector Graphics files to give them their full name, differ from standard image files such as BMP, JPG, and PNG files. Vector graphics are constructed using mathematical formulas that establish points on a grid, rather than specific blocks of color (pixels). The advantage of vector graphics files is that they can be scaled infinitely with no loss of resolution, something that cannot be done with pixel-based images. Vector files are often used for logos, as they can be scaled up easily to be used in billboards with no loss of resolution, and they are increasingly being used on the web as the images will display correctly regardless of the size of the browser window or screen.

SVG is an incredibly versatile file format that can incorporate elements other than the image code, for instance, SVG files can be used to display HTML. It is possible to create an SVG image file that incorporates HTML and executes JavaScript on loading, redirecting users to a malicious website such as a phishing landing page. Images can be created that incorporate clickable download buttons, which will download payloads from a remote URL. An end user could easily be tricked into downloading a file with a double extension that appears to be a PDF file but is actually a malware executable.

Some of the recently intercepted phishing emails have included an SVG file that displays an image of an Excel spreadsheet. Since the spreadsheet is an image, the user cannot interact with it, but it includes an embedded form that mimics the Microsoft 365 login prompt. If the user enters their credentials into that form, they are transmitted to the threat actor. One of the problems with this type of file format is it is not generally blocked by anti-spam software, so is likely to be delivered to inboxes.

While SVG and other vector graphics file formats are invaluable for design and can be found extensively on the web, they are not generally used for image sharing, so the easiest way to protect against these malicious campaigns is to configure your spam filtering service to block or quarantine emails containing SVG file attachments, at least for employees who do not usually work with these file formats. If you have a cloud-based anti-spam service that incorporates email sandboxing, where attachments are sent for deep analysis, it is possible to detect SVG files that incorporate malicious JavaScript. Since the use of these file formats is increasing, it is important to make your employees aware of the threat through security awareness training. Emails with SVG file attachments should also be incorporated into your phishing simulations to determine whether employees open these files. Both are easy with the SafeTitan security awareness training and phishing simulation platform.

DocuSign Abused in Massive Phishing Campaign

by G Hunt | November 28, 2024 | Phishing & Email Spam

A large-scale phishing campaign has been identified that abuses the e-signature software DocuSign, a hugely popular software solution used to legally and securely sign digital documents and eliminate the time-consuming process of manually signing documents.

DocuSign uses “envelopes” to send documents to individuals for signing. These document containers may contain one or more documents that need to be signed, and the envelopes are sent via email. In this campaign, a bad actor abuses the DocuSign Envelopes API to create fake invoices, which are mass-distributed via email. This campaign aims to get the recipient of the invoice to sign it using DocuSign, then the signed document can be used for the next phase of the scam, which typically involves sending the signed document to the billing department for payment, which may or may not be through DocuSign. The invoices generated for this campaign are based on legitimate DocuSign templates and are generated through a legitimate DocuSign account. The invoices include legitimate branding for DocuSign and the company/product the threat actor is impersonating – such as Norton Internet Security, PayPal, and other big-name brands.

The problem for businesses with this campaign is the emails are sent from the genuine docusign[.]net domain, which means email security solutions are unlikely to block the messages since the domain is trusted. Since the emails appear to be legitimate invoices with genuine branding and the correct invoice amount for the product being spoofed, end users are likely to be tricked by the emails. The tactics used in this campaign are similar to others that have abused legitimate cloud-based services to bypass email security solutions, such as sending malicious URLs in documents hosted on Google Docs and Microsoft SharePoint.

The primary defense against these campaigns is security awareness training. Businesses need to make their employees aware of campaigns such as these messages, which often bypass email security solutions and are likely to land in inboxes since they may not contain any malicious URLs or malware code and are sent from a legitimate, trusted domain. The workforce needs to be trained on cybersecurity best practices and told about the red flags in emails that are indicative of a scam. Training needs to be provided continuously to make employees aware of the latest scams, as bad actors are constantly refining their tactics, techniques, and procedures, and developing new ways to trick end users. The easiest way to do this is with a comprehensive security awareness training solution such as SafeTitan.

SafeTitan makes it easy to create training programs for different roles in the organization and automate these training programs to ensure training content is delivered in manageable chunks, with new content added and rolled out in response to the latest threats. These training programs should be augmented with phishing simulations. An email security solution with AI and machine-learning capabilities is also important, as standard spam software is not effective at identifying threats from legitimate and trusted cloud services. TitanHQ's PhishTitan solution for Microsoft 365 has these capabilities and identifies the phishing emails that Microsoft often misses. PhishTitan scans inbound messages for malicious content, uses email sandboxing for detecting zero-day threats, adds banners to emails from external sources, and allows security teams to rapidly remediate identified threats throughout the entire email environment. In November 2024, Virus Bulletin assessed the engine that powers the SpamTitan spam filtering service and PhishTitan anti-phishing solution using around 125,000 emails. SpamTitan and PhishTitan blocked 100% of malware and 100% of phishing emails and only miscategorized 2 benign spam emails, demonstrating how effective these solutions are at blocking malicious emails.

For more information on improving your defenses against malicious email campaigns through cutting-edge email security and security awareness training, give the TitanHQ team a call today.

Multifactor Authentication Can Give a False Sense of Security

by G Hunt | November 26, 2024 | Phishing & Email Spam, Spam Software

It is all too easy to place too much reliance on multifactor authentication (MFA) to protect against phishing attacks. In theory, if an employee is duped by a phishing email and their credentials are stolen, MFA should stop the threat actor from using those credentials to access the account, as they will not have the necessary additional authentication factor(s). The reality is somewhat different. While MFA can – and does – block many attacks where credentials have been obtained, it is far from infallible. MFA has made it much harder to compromise accounts but, in response, threat actors have developed new tactics to bypass MFA protections.

For example, there is a scam where an employee is contacted by an individual who claims to be from their IT department. The scammer tells them there is an issue with their account and they need to update their password. They are directed to a site where they are prompted to enter their password and enter the MFA code sent to their phone. The threat actor uses that information in real-time to access their account. Multiple campaigns have targeted IT helpdesk staff, with the threat actor impersonating an employee. They provide information to verify their identity (obtained in an earlier phase of the campaign) and ask to register a new device to receive their MFA codes.

Phishing-as-a-service toolkits (PhaaS) capable of defeating MFA are advertised on hacking forums and Telegram channels that can be purchased or rented. They involve an adversary-in-the-middle (AitM) attack and use a reverse proxy between the victim and the legitimate portal for the credentials being sought. The user is directed to a login page that appears exactly as expected, as the user is logging into the genuine site. What is unknown to the user is the attacker sits between them and the site and captures credentials and the session cookie after MFA is successfully navigated. The attacker then has access to the account for the duration of the session cookie and can register a new device to receive future codes.

PhaaS kits are a serious threat and are proving popular with cybercriminals. Take the Rockstar 2FA kit for example, which is advertised for $200 for a 2-week subscription. The kit includes everything a phisher needs, including MFA bypass, login pages for targeting specific credentials, session cookie harvesting, undetectable malicious (FUD) links and link redirectors, a host of phishing templates, and an easy-to-use admin panel that allows tracking of phishing campaigns. The phishing URLs available are also hosted on legitimate services such as Google Docs Viewer, Microsoft OneDrive, and LiveAgent – sites commonly trusted by email security solutions. This is just one phishing kit. There are many being offered with similar capabilities.

The take-home message is that MFA, while important, can be bypassed. For maximum protection, phishing-resistant multifactor authentication should be used – e.g. smartcards or FIDO security keys. These MFA tools can be expensive to implement, so at the very least ensure that you have some form of MFA implemented and implement several other layers of defenses. An advanced spam filtering service such as SpamTitan is essential, as it can block phishing emails to ensure they do not reach end users. Review sites often rate SpamTitan as one of the best spam filters for business due to how easy the solution is to use and its excellent detection rate. In November 2024, in tests by Virus Bulletin, SpamTitan blocked 100% of malware and 100% of phishing emails out of a test involving around 125,000 messages. Previous assessments had a catch rate of more than 99.99%, demonstrating the reliability and accuracy of the solution.

Another layer of protection can be provided by a web filter, which will block attempts to visit known malicious websites, such as those used for phishing and malware distribution. WebTitan provides time-of-click protection, as does TitanHQ's PhishTitan product – an anti-phishing solution specifically developed to protect M365 accounts against phishing by augmenting Microsoft's controls to catch the phishing emails that EOP and Defender miss.

Technical defenses are important, but so too is workforce training. Through regular security awareness training and phishing simulations, employees can be taught cybersecurity best practices and how to identify and avoid scam emails. If you want to improve your defenses against phishing and malware, give the TitanHQ team a call and have a chat about your options. All TitanHQ solutions are easy to use, are available on a free trial, and full product support is provided during that trial.

Excel File Attachments Used in Phishing Campaign to Deliver Fileless Remote Access Trojan

by G Hunt | November 15, 2024 | Phishing & Email Spam

A phishing campaign has been identified that uses purchase order-related lures and Excel file attachments to deliver the Remcos RAT, a commercially available malware variant that gives threat actors remote access to an infected device. The malware allows the threat actor to log keystrokes, record audio via the microphone, and take screenshots and provides a foothold allowing an extensive compromise. Infection with the Remcos RAT invariably involves data theft and could lead to a ransomware attack and extortion.

Businesses with antivirus software installed are unlikely to be protected. While antivirus software is effective at detecting and neutralizing malware, the Remcos RAT is poorly detected as it is fileless malware that runs in memory and does not install files on the disk. The campaign, detected by researchers at FortiGuard Labs, targets Windows users and starts with a phishing email with an encrypted Excel attachment. The emails purport to be a

purchase order and include a malicious Excel file attachment. The Excel file uses OLE objects to exploit an old vulnerability in Office, tracked as CVE-2017-0199. Successful exploitation of the vulnerability will see an HTML Application (HTA) file downloaded, which is launched using mshta.exe. The file is heavily obfuscated to evade security solutions, and its function is to download and execute a binary, which uses process hollowing to download and run the Remcos RAT in the memory.

The Remcos RAT is used to enumerate and terminate processes, execute commands, capture sensitive data, and download additional malware payloads. Since the Remcos RAT runs in the memory, it will not survive a reboot. To achieve persistence, it runs the registry editor (reg.exe) to edit the Windows Registry to add a new auto-run item to ensure it is launched after each reboot.

Since the initial contact is made via email, an advanced email security solution with email sandboxing and AI- and machine learning capabilities should ensure the email is identified as malicious and blocked to prevent delivery. Should the email be delivered and the attachment opened, end users are informed that the document is protected. They are presented with a blurred version of the Excel file and are told they need to enable editing to view the content – a red flag that should be identified by security-aware employees. If that red flag is missed, enabling content will trigger the exploitation of the vulnerability that ultimately delivers the Remcos RAT. Businesses with an advanced DNS-based web filter will have another layer of protection, as the URLs hosting the malicious files should be blocked.

TitanHQ offers cutting-edge cybersecurity solutions that provide exceptional protection against phishing, BEC, and malware attacks, blocking the initial emails and connections to malicious websites to prevent end users from viewing malicious emails (SpamTitan) and preventing malicious file downloads from the Internet (WebTitan). In November 2024 tests by Virus Bulletin, TitanHQ's SpamTitan Solution had a 100% phishing and malware block rate. TitanHQ also provides a comprehensive security awareness training platform (SafeTitan) to teach cybersecurity best practices and keep employees aware of the latest threats. The platform also incorporates a phishing simulator for reinforcing training. Give the TitanHQ team a call today for more information on TitanHQ solutions and how they can improve your defenses against email, web, SMS, and voice-based threats at your business.

A Russian APT Group is Conducting a Massive Spear Phishing Campaign

by G Hunt | October 31, 2024 | Phishing & Email Spam

The notorious Russian advanced persistent threat (APT) group Midnight Blizzard (aka Cozy Bear, APT29) has been conducting a massive spear phishing campaign on targets in the United Kingdom, Europe, Australia, and Japan. Midnight Blizzard is a hacking group with strong links to Russia's Foreign Intelligence Service (SVR) which engages in espionage of foreign interests and seeks persistent access to accounts and devices to steal information of interest to the SVR. The latest campaign is a highly targeted information-gathering exercise that was first observed on October 22, 2024.

While Midnight Blizzard's spear phishing attacks are usually conducted on government officials and individuals in non-governmental organizations (NGOs), individuals in academia and other sectors have also been targeted. The spear phishing attacks were identified by Microsoft Threat Intelligence which reports that thousands

of emails have been sent to more than 100 organizations and the campaign is ongoing. While spear phishing is nothing new, Midnight Blizzard has adopted a new tactic in these attacks and is sending a signed Remote Desktop Protocol (RDP) configuration file as an email attachment, with a variety of lures tailored to the individual being targeted. Some of the intercepted emails impersonated Microsoft, others impersonated cloud service providers, and several of the emails used lures related to zero trust. The email addresses used in this campaign have been previously compromised in other Midnight Blizzard campaigns.

Amazon has also reported that it detected phishing emails that impersonated Amazon Web Services (AWS), attempting to trick the recipients into thinking AWS domains were used; however, the campaign did not seek AWS credentials, as Midnight Blizzard is targeting Windows credentials. Amazon immediately started the process of seizing the domains used by Midnight Blizzard to impersonate AWS and that process is ongoing.

RDP files contain automatic settings and resource mappings and are created when a successful connection to an RDP server occurs. The attached RDP files are signed with a Lets Encrypt certificate and extend features and resources of the local system to a remote server under the attacker's control. If the RDP file is executed, a connection is made to a server under the control of Midnight Blizzard, and the targeted user's local device's resources are bidirectionally mapped to the server.

The server is sent resources including logical hard disks, clipboard contents, printers, connected devices, authentication features, and Windows operating system facilities. The connection allows the attacker to install malware, which is set to execute via AutoStart folders, steal credentials, and download other tools to the user's device, including remote access trojans to ensure that access to the targeted system is maintained when the RDP session is closed.

Since the emails were sent using email addresses at legitimate organizations, they are unlikely to be flagged as malicious based on reputation checks by anti-spam software, although may be detected by more advanced anti-spam services that incorporate machine learning and AI-based detection mechanisms and email sandboxing. You should configure your spam antivirus filter to block emails containing RDP files and other executable files and configure your firewall to block outbound RDP connection attempts to external or public networks. Multifactor authentication should be configured on all accounts to prevent compromised credentials from granting access, and consider blocking executable files from running via your endpoint security software is the executable file is not on a trusted list. Also, ensure that downloaded files are scanned using antivirus software. A web filter can provide added protection against malicious file downloads from the internet.

An anti-phishing solution should also be considered for augmenting the protection provided through Microsoft Defender and EOP for Microsoft 365. PhishTitan from TitanHQ has been shown to improve protection and block threats that Microsoft's anti-phishing solution fails to detect, augmenting rather than replacing the protection provided by EOP and Defender. It is also important to provide security awareness training to the workforce and ensure that spear phishing and RDP file attachments are included in the training. Also, consider conducting spear phishing simulations.

Malvertising Campaign Uses Facebook Ads to Deliver SYS01 Information Stealer

by G Hunt | October 30, 2024 | Internet Security

A new malvertising campaign has been identified that abuses the Meta advertising platform to deliver an information stealer malware variant called SYS01 Stealer. Similar to other malvertising campaigns, popular brands are impersonated to trick users into downloading the information stealer in the belief they are installing legitimate software. In this campaign, the impersonated brands include popular software tools that are commonly used by businesses, including the video and imaging editing tools CapCut, Adobe Photoshop, and Canva, as well as productivity tools such as Office 365, instant messaging platforms such as Telegram, VPN providers such as Express VPN, and a host of other software products and services to ensure a wide reach, including video games and streaming services.

The adverts claim that these software solutions games and services are available free of charge, which is a red flag as the genuine products and services usually require a purchase or subscription. The advertisements are published via hijacked Facebook business accounts, which according to an analysis by Bitdefender, have been used to create thousands of ads on the platform, many of which remain active for months. If a user interacts with one of the adverts, they are directed to sites hosted on Google Sites or True Hosting. Those sites impersonate trusted brands and offer the application indicated in the initial ad. If the user is tricked and progresses to a download, a zip file is delivered that contains an executable file that sideloads a malicious DLL, which launches the infection process.

The DLL will run PowerShell commands that will prevent the malware from executing in sandboxes and will prepare the environment for the malware to be installed, including disabling security solutions to ensure the malware is not detected, and maintaining persistence ensured through scheduled tasks. Some identified samples include an Electron application with JavaScript code embedded that drops and executes the malware.

The cybercriminals behind the campaign respond to detections of the malware by security solutions and change the code when the malware starts to be blocked, with the new variant rapidly pushed out via Facebook ads. The information stealer primarily targets Facebook business accounts and steals credentials allowing those accounts to be hijacked. Personal data is stolen, and the accounts are used to launch more malicious ads. Since legitimate Facebook business accounts are used, the attackers can launch malicious ads at scale without arousing suspicion. This malvertising campaign stands out due to its scale, with around 100 malicious domains currently used for malware distribution and command and control operations.

Businesses should take steps to ensure they are protected by using a web filter to block the malicious domains used to distribute the malware, the Facebook site for employees, and to prevent malware downloads from the Internet. Since business Facebook accounts are targeted, it is important to ensure that 2-factor authentication is enabled in the event of credentials being compromised and business Facebook accounts should be monitored for unauthorized access. Business users should not install any software unless it comes from an official source, which should be reinforced through security awareness training.

TitanHQ has developed an easy-to-use web filter called WebTitan that is constantly updated with threat intelligence to block access to malicious sites as soon as they are discovered. WebTitan can be configured to block certain file downloads from the Internet by extension to reduce the risk of malware infections and control shadow IT, and WebTitan makes it easy for businesses to enhance productivity while improving security by blocking access to known distractions such as social media platforms and video streaming sites. WebTitan provides real-time protection against clicks in phishing emails by preventing a click from launching a malicious website and the solution can be used to protect all users on the network as well as off-network users on portable devices through

the WebTitan on-the-go roaming agent. For more information about improving your defenses against malware delivered via the internet and malvertising campaigns, give the TitanHQ team a call today.

TitanHQ Launches Security Awareness Training for MSPs

by G Hunt | October 26, 2024 | Security Awareness

Managed service providers can implement security solutions to protect their clients from phishing, social engineering, and business email compromise attacks but if a malicious email manages to bypass those defenses, it could easily result in hackers gaining a foothold in the network, resulting in a highly disruptive and costly cyberattack and data breach. To improve defenses against phishing, managed service providers should offer their clients security awareness training to manage human risk, and now TitanHQ can offer a security awareness training (SAT) solution that allows them to do that with ease.

This month, TitanHQ launched its Security Awareness Training (SAT) solution for MSPs. The solution has been specifically created to be used by MSPs and allows them to provide affordable, scalable training with minimal setup. The training platform has now been integrated with TitanHQ's MSP cybersecurity platform and is ready for MSPs to use. In contrast to many SAT solutions that only provide standard cybersecurity training, TitanHQ's SAT solution integrates advanced phishing simulation with behavior-focused training that is fun and engaging for participants. The solution delivers maximum value to MSPs and can be rapidly set up, allowing them to roll out training programs to new clients with just a few clicks. There is no need to spend hours assigning training content to new customers, as it is possible to select multiple customers and rapidly spin up training courses that can be rapidly deployed for individuals or groups of customers in the future.

The AI-driven training platform allows training content to be tailored to individual employees to meet their training needs, personalizing the training experience. The platform includes more than 80 videos, training sessions, and webinars to improve awareness and help create a security culture. MSPs are provided with monthly reports on the progress that is being made by individual employees and they are provided with actionable insights.

The platform includes a phishing simulator that allows MSPs to conduct real-time phishing simulations based on a huge variety of templates (1,800+) covering all types of phishing and other attack scenarios, and the content is updated regularly to include the latest tactics, techniques, and procedures used by cybercriminals in real-world phishing campaigns. MSPs can easily pre-configure phishing simulations and training campaigns to roll out to new clients as they are onboarded, and the MSP dashboard provides a view of quick actions and live analytics all in one place.

The training platform can deliver reactive training in response to user behavior, where users in need of training are automatically enrolled and delivered relevant training content. MSPs can use the platform to conduct cyber awareness knowledge checks to identify areas where individuals need training, verify understanding of the training material, and retest employees over time to ensure they have not forgotten the material from previous training sessions. The training material covers the cyber threats that employees are likely to encounter such as phishing, social engineering, business email compromise, and malware, but also in-person threats such as physical security, ensuring they receive comprehensive training that covers all the bases.

If you have yet to start offering security awareness training to your clients, or if you already offer training but require a more comprehensive and easier-to-use training platform, give the TitanHQ team a call. Product demonstrations can be arranged on request to show you just how easy the platform is to use.

“Our integrated cybersecurity platform delivers maximum value to MSPs, offering a quicker time-to-market, reduced set-up requirements combined with real-world, practical security awareness training & phishing simulations. TitanHQ delivers that seamlessly, allowing MSPs to offer comprehensive SAT to their customers in just a few clicks,” said TitanHQ CEO, Ronan Kavanagh.

Multiple Accounts Compromised in Targeted Phishing Campaigns

by G Hunt | October 26, 2024 | Phishing & Email Spam

The purpose of phishing attacks is usually to steal credentials to gain unauthorized access to accounts. If an employee falls for a phishing attack and their credentials are obtained, the attacker can gain access to that user’s account and any data contained therein. That access can be all that is required for the threat actor to achieve a much more extensive compromise.

Oftentimes, a threat actor conducts a more extensive phishing campaign on multiple employees at the same organization. These phishing attacks can be harder to spot as they have been tailored to that specific organization. These attacks usually spoof an internal department with the emails seemingly sent from a legitimate internal email account. The emails may address each individual by name, or appear to be broadcast messages to staff members. One successful campaign was identified by the Office of Information Technology at Boise State University, although not before several employees responded to the emails and disclosed their credentials. In this campaign, the emails were addressed to “Dear Staff,” and appeared to have been sent from the postmaster account by “Health Services,” purporting to be an update on workplace safety. The emails had the subject line “Workplace Safety: Updates on Recent Health Developments,” with a similar campaign indicating a campylobacter infection had been reported to the health department.

In the message, recipients were advised about a health matter involving a member of staff, advising them to contact the Health Service department if they believed they had any contact with the unnamed worker. In order to find out if they had any contact with the worker, the link must be clicked. The link directed the user to a fraudulent login page on an external website, where they were required to enter their credentials. The login page had been created to look like it was a legitimate Boise State University page, captured credentials, and used a Duo Securit notification to authorize access to their account.

These targeted campaigns are now common, especially at large organizations where it is possible to compromise a significant number of accounts and is worth the attacker’s time to develop a targeted campaign. Another attack was recently identified by the state of Massachusetts. The attacker created a fake website closely resembling the HR/CMS Employee Self-Service Time and Attendance (SSTA) system, which is used for payroll. Employees were tricked into visiting the portal and were prompted to enter their credentials, which the attacker used to access their personal and direct deposit information. In this case, the aim of the attack appeared to be to change direct deposit information to have the employees’ wages paid into the attacker’s account. Several employees were fooled by the

scam; although in this case the attack was detected promptly and the SSTA system was disabled to prevent fraudulent transfers.

A different type of campaign recently targeted multiple employees via email, although the aim of the attack was to grant the threat actor access to the user's device by convincing them to install the legitimate remote access solution, AnyDesk. The threat actor, the Black Basta ransomware group, had obtained employee email addresses and bombarded them with spam emails, having signed them up for newsletters via multiple websites. The aim was to create a legitimate reason for the next phase of the attack, which occurred via the telephone, although the group has also been observed using Microsoft Teams to make contact. The threat actor posed as the company's IT help desk and offered assistance resolving the spam problem they created, which involved downloading AnyDesk and granting access to their device. During the session, tools are installed to provide persistent access. The threat actor then moved laterally within the network and extensively deployed ransomware.

These attacks use social engineering to exploit human weaknesses. In each of these attacks, multiple red flags should have been spotted revealing these social engineering attempts for what they are but more than one employee failed to spot them. It is important to provide security awareness training to the workforce to raise awareness of phishing and social engineering threats, and for training to be provided regularly. Training should include the latest tactics used by threat actors to breach networks, including phishing attacks, fake tech support calls, malicious websites, smishing, and vishing attacks.

A phishing simulator should be used to send realistic but fake phishing emails internally to identify employees who fail to spot the red flags. They can then receive additional training relative to the simulation they failed. By providing regular security awareness training and conducting phishing simulations, employers can develop a security culture. While it may not be possible to prevent all employees from responding to a threat, the severity of any compromise can be limited. With TitanHQ's SafeTitan solution, it is easy to create and automate tailored training courses and phishing simulations that have been shown to be highly effective at reducing susceptibility to phishing and other threats.

Since threat actors most commonly target employees via email, it is important to have robust email defenses to prevent the threats from reaching employees. Advanced anti-spam services such as SpamTitan incorporate a wide range of threat detection methods to block more threats, including reputation checks, extensive message analysis, machine-learning-based detection, antivirus scans, and email sandboxing for malware detection. SpamTitan has been shown to block more than 99.99% of phishing threats and 100% of malware.

TOAD Attacks: New Voice-Based Phishing Techniques Used in Attacks on Businesses

by G Hunt | October 24, 2024 | Phishing & Email Spam

Phishing is one of the most effective methods used by cyber actors to gain initial access to protected networks Phishing tactics are evolving and TOAD attacks now pose a significant threat to businesses. TOAD stands for Telephone-Oriented Attack Delivery and is a relatively new and dangerous form of phishing that involves a telephone call, although there are often several different elements to a TOAD attack which may include initial contact via email, SMS messages, or instant messaging services.

TOAD attacks often start with an information-gathering phase, where the attacker obtains personal information about individuals that can then be targeted. That information may only be a mobile phone number or an email address, although further information is required to conduct some types of TOAD attacks.

One of the most common types of TOAD attacks is callback phishing. The attacker impersonates a trusted entity in an email and makes a seemingly legitimate request to make contact. There is a sense of urgency to get the targeted individual to take prompt action. Rather than use a hyperlink in the message to direct the user to a website, the next phase of the attack takes place over the telephone or a VOIP-based service such as WhatsApp. A phone number is included that must be called to resolve a problem.

If the call is made, the threat actor answers and during the call, trust is built with the caller and the threat actor makes their request. That could be an instruction to visit a website where sensitive information must be entered or a file must be downloaded. That file download leads to a malware infection.

Several TOAD attacks have involved the installation of legitimate remote access software. One campaign involved initial contact via email about an expensive subscription that was about to be renewed, which required a call to cancel. The threat actor convinces the user to download remote access software which they are told is necessary to prevent the charge being applied, such as to fully remove the software solution from the user's device.

The user is convinced to give the threat actor access to their device through the software and the threat actor keeps the person on the line while they install malware or perform other malicious actions, reassuring them if they get suspicious. Other scams involve initial contact about a fictitious purchase that has been made, or a bank scam, where an email impersonates a bank and warns the victim that an account has been opened in their name or a large charge is pending. These attacks result in the victim providing the threat actor with the information they need to access their account.

TOAD attacks often involve the impersonation of a trusted individual, who may be a colleague, client, or even a family member. Since information is gathered before the scam begins, when the call is made, the threat actor can provide that information to the victim to convince them that they are who they claim to be. That information may have been purchased on the dark web or obtained in a previous data breach. For instance, following a healthcare data breach, the healthcare provider may be impersonated, and the attacker can provide medical information in their possession to convince the victim that they work at the hospital.

The use of AI tools makes these scams even more convincing. Deepfakes are used, where a person's voice is mimicked, or video images are manipulated on video conferencing platforms. Deepfakes were used in a scam on an executive in Hong Kong, who was convinced to transfer around £20 million in company funds to the attacker's account, believing they were communicating with a trusted individual via a video conferencing platform.

TOAD attacks may be solely conducted over the phone, where the attacker uses call spoofing to manipulate the caller ID to make it appear that the call is coming from a known and previously verified number. Other methods may be used to convince the victim that the reason for the call is genuine, such as conducting a denial-of-service attack to disrupt a service or device to convince the user that there is an urgent IT problem that needs to be resolved. TOAD attacks are increasing because standard phishing attacks on businesses are becoming harder to

pull off due to email security solutions, multifactor authentication, and improved user awareness about scam messages.

Unfortunately, there is no single cybersecurity solution or method that can combat these threats. A comprehensive strategy is required that combines technical measures, security awareness training and administrative controls. Advanced anti-spam software with machine learning and AI-based detection can identify the emails that are used for initial contact. These advanced detection capabilities are needed because the initial emails often contain no malicious content, other than a phone number. SpamTitan, TitanHQ's cloud-based anti-spam service, can detect these initial emails through reputation checks on the sender's IP address, email account, and domain, and machine learning is used to analyze the message content, including comparing emails against the typical messages received by a business.

WebTitan is a cloud-based DNS filter that is used to control the web content that users can access. WebTitan will block access to known malicious sites and can be configured to prevent certain file types from being downloaded from the internet, such as those commonly used to install malware, unauthorized apps, and remote access solutions.

Regular security awareness training is a must. All members of the workforce should be provided with regular security awareness training and TOAD attacks should feature in the training content. SafeTitan, TitanHQ's security awareness training platform and phishing simulator, makes it easy for businesses to create and automate training courses for the workforce. Employees should be trained in how to identify a TOAD attack, told not to trust caller ID alone, to avoid clicking links in emails and SMS messages, and to be vigilant when receiving or making calls, and to report any suspicious activity and immediately end a call if something does not seem right.

Mamba 2FA Phishing Kit Used to Bypass MFA on Microsoft 365 Accounts

by G Hunt | October 20, 2024 | Phishing & Email Spam

Researchers have identified a new phishing kit that is being used to steal credentials for Microsoft 365 accounts and gain access to accounts protected by multi-factor authentication (MFA). The phishing kit, called Mamba 2FA is a cause of concern as it has the potential to be widely adopted given its relatively low price and there are signs it is proving popular with cybercriminals since its release in late 2023. Phishing kits make it easy for low-skilled cybercriminals to conduct sophisticated attacks as they provide all the tools required to breach accounts. The Mamba 2FA kit includes the necessary infrastructure to conduct phishing campaigns, masks IP addresses to prevent them from being blocked, and updates the phishing URLs frequently to ensure they remain active and are not blocked by security solutions.

The Mamba 2FA kit includes phishing pages that mimic Microsoft services such as OneDrive and SharePoint, and the pages can be customized to create realistic phishing URLs for targeting businesses, including allowing the business logo and background images to be added to the login page. Since businesses often have MFA enabled, simply stealing Microsoft credentials is not sufficient, as the MFA will block any attempt to use the credentials for unauthorized access. Like several other popular phishing kits, the Mamba 2FA kit supports adversary-in-the-middle (AitM) attacks, incorporating proxy relays to steal one-time passcodes and authentication cookies in real time. When credentials are entered into the phishing page, they are relayed to Microsoft's servers in real-time and

Microsoft's responses are relayed back to the victim, including MFA prompts, which allows the threat actor to steal the session cookie and gain access to the user's account.

Phishing kits such as Mamba 2FA pose a serious threat to businesses, which should take steps to protect against attacks. The AitM tactics can defeat less secure forms of MFA that are based on one-time passwords but are not effective against hardware-based MFA. Implementing phishing-resistant MFA will ensure these attacks do not succeed. Other recommended controls include geo-blocking and allowlisting for IPs and devices. While these advanced phishing kits are effective, threat actors must convince people to click a link in an email and disclose their login credentials, and with advanced email security solutions these phishing threats can be identified and blocked before they reach inboxes. Training should also be provided to the workforce to help with the identification and avoidance of phishing.

TitanHQ can help through the SpamTitan cloud-based spam filtering service and the SafeTitan security awareness training and phishing simulation platform. SpamTitan incorporates reputation checks, Bayesian analysis, greylisting, machine learning-based detection, antivirus scans, and email sandboxing to block phishing and malware threats. Independent tests demonstrated SpamTitan was one of the best spam filtering solutions for businesses at blocking threats, with a 99.99% phishing block rate and a 100% malware block rate.

The SafeTitan security awareness training platform makes it easy for businesses to provide regular cybersecurity awareness training. The platform includes more than 80 training modules, videos, and webinars, with hundreds of phishing simulation templates based on real-world phishing examples. Regular training and phishing simulations have been proven to be highly effective at reducing susceptibility to phishing and other threats targeting employees. This month, TitanHQ has also launched its security awareness training platform for MSPs, which has been specifically developed to make it quick and easy for MSPs to incorporate security awareness training into their service stacks. Speak with TitanHQ today for more information about these and other cybersecurity solutions for combatting the full range of cyber threats.

Cyber Actors Conducting Spear Phishing Campaigns for Iranian State

by G Hunt | September 30, 2024 | Internet Security, Network Security

Spear phishing attacks are being conducted by a cyber threat group working on behalf of Iran's Islamic Revolutionary Guard Corps. The cyber threat actors have been gaining access to the personal and business accounts of targeted individuals to obtain information to support Iran's information operations.

According to a joint cybersecurity advisory issued by the Federal Bureau of Investigation (FBI), U.S. Cyber Command – Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury), and the United Kingdom's National Cyber Security Centre (NCSC), the campaign has been targeting individuals with a nexus to Iranian and Middle Eastern affairs, including journalists, political activists, government officials, think tank personnel, and individuals associated with US political campaign activity.

Individuals are typically contacted via email or messaging platforms. As is common in spear phishing attacks, the cyber threat actors impersonate trusted contacts, who may be colleagues, associates, acquaintances, or family members. In some of the group's attacks, they have impersonated known email service providers, well-known journalists seeking interviews, contacts offering invitations to conferences or embassy events, or individuals

offering speaking engagements. There have been instances where an individual is impersonated who is seeking foreign policy discussions and opinions.

In contrast to standard phishing attacks where the victim is sent a malicious email attachment or link to a phishing website in the initial email, more effort is put into building a rapport with the victim to make them believe they are engaging with the person the scammer is impersonating. There may be several exchanges via email or a messaging platform before the victim is sent a malicious link, which may be embedded in a shared document rather than being directly communicated via email or a messaging app.

If the link is clicked, the victim is directed to a fake email account login page where they are tricked into disclosing their credentials. If entered, the credentials are captured and used to login to the victim's account. If the victim's account is protected with multi-factor authentication, they may also be tricked into disclosing MFA codes. If access to the account is gained, the cyber threat actor can exfiltrate messages and attachments, set up email forwarding rules, delete or manipulate messages, and use the account to target other individuals of interest.

Spear phishing attempts are harder to identify than standard phishing attempts as greater effort is put in by the attackers, including personalizing the initial contact messages, engaging in conversations spanning several messages, and using highly plausible and carefully crafted lures. These emails may bypass standard spam filtering mechanisms since the emails are not sent in mass campaigns and the IP addresses and domains used may not have been added to blacklists.

It is important to have robust anti-phishing, anti-spam, and anti-spoofing solutions in place to increase protection and prevent these malicious emails from reaching their intended targets. An advanced spam filtering solution should be used that incorporates Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) to identify spoofing and validate inbound emails. SpamTitan also incorporates machine learning and AI-based detection to help identify spear phishing attempts.

If you are a Microsoft 365 user, the anti-spam and anti-phishing mechanisms provided by Microsoft should be augmented with a third-party anti-phishing solution. PhishTitan can detect the spear phishing emails that Microsoft's EOP and Defender often miss while adding a host of detection mechanisms and anti-phishing features including adding banners to emails from external sources.

One of the main defenses against these attacks is vigilance. An end-user security awareness training program should be implemented to improve awareness of spear phishing attacks. SafeTitan makes this as easy as possible and covers all possible attack scenarios, with training provided in short and easy-to-assimilate training modules. It is also important to conduct phishing simulations to raise and maintain awareness. These simulations can be especially effective at raising awareness about spear phishing emails and giving end users practice at identifying these threats.

Multifactor authentication should be enabled on all accounts, with phishing-resistant multi-factor authentication providing the highest degree of protection. IT teams should also consider prohibiting email forwarding rules from automatically forwarding emails to external addresses and conducting regular scans of the company email server to identify any custom rules that have been set up or changes to the configuration. Alerts should also be configured for any suspicious activity such as logins from foreign IP addresses.

School Cyberattacks Increase 55% with Phishing Attacks the Most Common Threat

by G Hunt | September 30, 2024 | Security Awareness

While no sector is immune to cyberattacks, some sectors are targeted more frequently than others and attacks on the education sector are common and on the rise. In May 2024, new data released by the UK's Information Commissioner's Office revealed there had been 347 cyber incidents reported by the education and childcare sector in 2023, an increase of 55% from the previous year.

These attacks can prevent access to IT systems, forcing schools to resort to manual processes for checking pupil registers, teaching, and all other school functions. Without access to IT systems, teachers are unable to prepare for lessons, schools have been prevented from taking payment for pupil lunches, and many have lost students' coursework. The impact on schools, teachers, and students can be severe. Some schools have been forced to temporarily close due to a cyberattack.

A survey conducted by the Office of Qualifications and Examinations Regulation (Ofqual) found that 9% of surveyed headteachers had experienced a critically damaging cyberattack in the past academic year. 20% of schools were unable to immediately recover from a cyberattack and 4% reported that they still had not returned to normal operations more than half a term later.

The Ofqual survey revealed more than one-third of English schools had suffered a cyber incident in the past academic year and a significant percentage faced ongoing disruption due to a cyberattack. Cyberattacks can take many forms and while ransomware attacks are often the most damaging, the most common type of cyber incident is phishing. According to the survey, 23% of schools and colleges in England experienced a cybersecurity incident as a result of a phishing attack in the past year.

Schools are not sufficiently prepared to deal with these attacks. According to the survey, 1 in 3 teachers said they had not been provided with cybersecurity training in the past year, even though cybersecurity training has proven to be effective at preventing cyberattacks. The survey revealed that out of the 66% of teachers who had been provided with training, two-thirds said it was useful.

TitanHQ has developed a comprehensive security awareness training platform for all sectors, that is easy to tailor to meet the needs of individual schools. The platform includes an extensive range of computer-based training content, split into modules of no more than 10 minutes to make it easy for teachers and other staff members to complete. The training material is enjoyable, covers the specific threats that educational institutions face, and teaches the cybersecurity practices that can help to improve defenses and combat phishing, spear phishing, and malware attacks.

The SafeTitan platform also includes a phishing simulator for conducting simulated phishing attacks to improve awareness, reinforce training, and give staff members practice in identifying phishing and other cyber threats. The training and simulations can be automated, and training modules can be set to be triggered by security errors and risky behaviors. Further, the platform is affordable.

To find out more about improving human defenses at your educational institution through SafeTitan, give the TitanHQ team a call. TitanHQ can also help with improving technical defenses, with a suite of cybersecurity solutions for the education sector including SpamTitan anti-spam software, the PhishTitan anti-phishing solution, and the WebTitan DNS-based web filter. Combined, these technical defenses can greatly improve your security posture and prevent cyber threats them from reaching end users and their devices.

Ransomware Attacks Often Start with Malware Infections or Phishing Attacks

by G Hunt | September 15, 2024 | Network Security

Ransomware attacks can cause an incredible amount of damage to an organization's reputation as well as huge financial losses from the downtime they cause. Recovery from an attack, regardless of whether the ransom is paid, can take weeks and the theft and publication of sensitive data on the dark web can prompt customers to leave in their droves. Attacks are still being conducted in high numbers, especially in the United States and the United Kingdom. One recent survey indicates that 90% of businesses in those countries have experienced at least one attack in the past 12 months, with three-quarters of organizations suffering more than one attack in the past year.

The healthcare sector is often attacked as defenses are perceived to be weak and sensitive data can be easily stolen, increasing the chance of the ransom being paid. The Inc Ransom group has been targeting the healthcare sector and conducted an attack on an NHS Trust in Scotland earlier this year, stealing 3 TB of sensitive data and subsequently publishing that data on the dark web when the ransom wasn't paid.

The Inc Ransom group also conducted an attack on a Michigan healthcare provider, preventing access to its electronic medical record system for 3 weeks in August. A group called Qilin attacked an NHS pathology provider, Synnovis, in June 2024 which had a huge impact on patient services, causing a shortage of blood in London hospitals that caused many surgeries to be postponed. Education is another commonly attacked sector. The Billericay School in Essex had its IT system encrypted, forcing the school to temporarily close. In all of these attacks, highly sensitive data was stolen and held to ransom. The public sector, healthcare, and schools are attractive targets due to the value of the sensitive data they hold, and attacks on businesses cause incredibly costly downtime, both of which can force victims into paying ransoms. What is clear from the reporting of attacks is no sector is immune.

There is increasing evidence that ransomware groups are relying on malware for initial access. Microsoft recently reported that a threat actor tracked as Vanilla Tempest (aka Vice Society) that targets the healthcare and education sectors has started using Inc ransomware in its attacks and uses the Gootloader malware downloader for initial access. A threat actor tracked as Storm-0494 is responsible for the Gootloader infections and sells access to the ransomware group. Infostealer malware is also commonly used in attack chains. The malware is installed by threat groups that act as initial access brokers, allowing them to steal credentials to gain access to networks and then sell that access to ransomware groups. Phishing is also commonly used for initial access and is one of the main initial access vectors in ransomware attacks, providing access in around one-quarter of attacks.

Infostealer malware is often able to evade antivirus solutions and is either delivered via malicious websites, drive-by malware downloads, or phishing emails. Gootloader infections primarily occur via malicious websites, with malvertising used to direct users to malicious sites where they are tricked into downloading and installing

malware. Credentials are commonly compromised in phishing attacks, with employees tricked into disclosing their passwords by impersonating trusted individuals and companies.

Advanced cybersecurity defenses are needed to combat these damaging cyberattacks. In addition to traditional antivirus software, businesses need to implement defenses capable of identifying the novel malware threats that antivirus software is unable to detect. One of the best defenses is an email sandbox, where emails are sent for behavioral analysis. In the sandbox – an isolated, safe environment – file attachments are executed, and their behavior is analyzed, rather than relying on malware signatures for detection, and links are followed to identify malicious content.

DNS filters are valuable tools for blocking web-based delivery of malware. They can be used to control access to the Internet, prevent malvertising redirects to malicious websites, block downloads of dangerous file types from the Internet, and access to known malicious URLs. Employees are tricked into taking actions that provide attackers with access to their networks, by installing malware or disclosing their credentials in phishing attacks, so regular security awareness training is important along with tests of knowledge using phishing simulations.

There is unfortunately no silver bullet when it comes to stopping ransomware attacks; however, that does not mean protecting against ransomware attacks is difficult for businesses. TitanHQ offers a suite of easy-to-use cybersecurity solutions that provide cutting-edge protection against ransomware attacks. TitanHQ's award-winning products combine advanced detection such as email sandboxing, AI and machine-learning-based detection, and are fed threat intelligence from a massive global network of endpoints to ensure businesses are well protected from the full range of threats.

Give the TitanHQ team a call today and have a chat about improving your defenses with advanced anti-spam software, anti-phishing protection, DNS filtering, and security awareness training solutions and put the solutions to the test on a free trial to see for yourself the difference they make.

Is Your Business Protected Against Internal Phishing Attempts?

by G Hunt | August 29, 2024 | Phishing & Email Spam, Security Awareness

If a phishing attempt is successful and a threat actor gains access to an employee's email account, it is common for the compromised email account to be used for internal phishing. Some malware variants also allow threat actors to hijack email accounts and send malware internally, adding a copy of the malware to a message thread to make it appear that a file was attached in response to a past email conversation.

There are several different scenarios where these types of attacks will occur such as business email compromise attacks to gain access to an email account that can be used for the scam – a CEO, executive, HR, or IT department account for example; to distribute malware extensively to compromise as many accounts as possible; to gain access to multiple email accounts, or to compromise multiple accounts to gain access to sensitive data.

In industries where data breach reporting is mandatory, such as in healthcare in the United States, email account breaches are regularly reported where unauthorized activity is detected in a single email account, and the subsequent investigation reveals multiple employee email accounts have been compromised through internal phishing.

Internal phishing attempts are much harder to identify than phishing attempts from external email accounts. Even when email security solutions incorporate outbound scanning, these phishing attempts are often not recognized as malicious as the emails are sent from a trusted account. The recipients of these emails are also much more likely to trust an internal email than an external email from an unknown sender and open the email, click a link, or open a shared file.

Attackers may also spoof an internal email account. It is easy to find out the format used by a company for their emails, and names can be found on professional networking sites. A good email security solution should be able to identify these spoofed emails, but if they arrive in an inbox, an employee may be fooled into thinking that the email is a genuine internal email.

It is important for businesses to take steps to combat internal phishing as it is a common weak point in email defenses. Unfortunately, there is no single technical control that can protect against these phishing attempts. What is required is a combination of measures to provide layered protection. With layered security, if one measure fails to protect against a threat, others are in places that can thwart the attempt.

The best place to start is with a technical measure to identify and block these phishing threats. Spam filter software naturally needs to have inbound as well as outbound scanning; however, standard checks such as reputation scans are not enough. An email security solution should have AI and machine learning capabilities for assessing how emails deviate from standard emails sent internally and for in-depth analysis of message content. Link scanning is also important, with URL rewriting to identify the true destination of embedded URLs, OLE detection, and email sandboxing to identify malicious attachments – not just malware but also malicious links in email attachments.

Security awareness training is vital as employees may not be aware of threats they are likely to encounter. Security awareness training should include internal phishing and employees should be made aware that they should not automatically trust internal emails as they may not be what they seem. Security awareness training should be accompanied by phishing simulations, including simulated phishing attempts from internal email accounts. These will give employees practice in identifying phishing and security teams will learn how susceptible the workforce is and can then take steps to address the problem.

Multi-factor authentication is required. If a phishing attempt is not identified by either a security solution or the employee, and the employee responds and divulges their credentials, they can be used by the threat actor to access the employee's email account. Multi-factor authentication protects against this by requiring another factor – in addition to a password – to be provided. The most robust form of MFA is phishing-resistant MFA, although any form of MFA is better than none.

TitanHQ can help protect against phishing attacks of all types through the SpamTitan cloud-based spam filtering service, the PhishTitan anti-phishing solution for M365, and the SafeTitan Security awareness training and phishing simulation platform.

The engine that powers SpamTitan and PhishTitan has an exceptional phishing catch rate, including internal phishing attempts. The engine incorporates AI- and machine learning algorithms that can detect novel phishing attempts and emails that deviate from the normal emails sent internally, as well as OLE detection, URL rewriting, and email sandboxing for catching novel malware and phishing threats.

The SafeTitan Security awareness training platform includes an extensive library of training content to teach security best practices, eradicate risky behaviors, and train employees on how to recognize an extensive range of threats. The phishing simulator makes it easy to conduct internal phishing tests on employees to test knowledge and give employees practice at identifying email threats. Usage data shows the platform can reduce employee susceptibility to phishing attempts by up to 80%.

For more information about improving your phishing defenses, speak with TitanHQ today.

Common Phishing Examples That Employees Fall For

by G Hunt | August 28, 2024 | Spam Software

Phishing is the name given to a type of cyberattack where the threat actor uses deception to trick an individual into taking an action that benefits the threat actor. A lure is used to get the targeted individual to respond and these attacks typically create a sense of urgency. Urgency is required as phishers need users to act quickly rather than stop and think about the request. The faster the response, the less time there is to identify the scam for what it is. There is often a threat to help create a sense of urgency, such as negative consequences if no action is taken.

Phishing can take place over the phone, SMS, and instant messaging platforms, but email is the most common way of getting the phishing lure in front of an employee. It is now common for businesses to provide security awareness training to the workforce to raise awareness of phishing threats and to have a spam email filter in place to detect and quarantine these malicious emails before they reach inboxes; however, even with robust defenses in place, some malicious emails will arrive in inboxes and employees are often tricked into responding.

Security awareness training programs teach employees to stop and think before taking any request in an email, which is the last thing phishers want the recipients of their emails to do. One of the ways they can get a quick response is to make the recipient believe that the email has been sent from an internal email account, either through spoofing or by using a compromised internal email account. Some of the lures used in phishing attempts that the majority of employees will at least open and read, are detailed below.

HR Themed Phishing Emails

One of the ways that phishers increase the chance of a user responding is to use Human Resources (HR)-themed lure, as any communication from the HR department is usually taken seriously by employees. These phishing attempts include the types of notifications that HR departments often send via email, examples of which include:

- Changes to working hours
- Updates to working practices
- Dress code changes
- Upcoming training/cybersecurity training sessions
- Annual leave notifications
- Payroll information requests
- Tax matters
- Healthcare and wellness benefit updates
- Employee rewards programs

- Notifications about disciplinary procedures

IT Department Notifications

Notifications from the IT department are also common as employees typically open these emails and act quickly. These include:

- Internet activity reports
- Security alerts
- The discovery of unauthorized software
- Changes to access rights
- Requires software installations

Notifications from Board Members

Phishers often impersonate the CEO or other executives, as they know that employees will want to respond quickly and are unlikely to question requests from these authority figures. CEOs are commonly impersonated in business email compromise attacks, where the threat actor tries to get an employee to make a wire transfer to their account, purchase gift cards, or divulge sensitive information. These emails may include a hyperlink to a website where the user is told they must enter their login credentials, a hyperlink to a website where a file download takes place, or the emails may include an attachment. Common file types used in these email campaigns include PDF files, HTML attachments, Office files, and compressed files. These files may contain malware or malicious scripts, or may be used to hide information from spam filtering software. For example, PDF files are commonly used that contain malicious links. By adding the link to the PDF file, there is less chance that spam filtering software will find and follow the link.

How to Defend Against These Common Email Threats

Defending against email attacks requires advanced anti spam software and regular security awareness training for the workforce. SpamTitan from TitanHQ is an advanced cloud-based anti-spam service that performs comprehensive checks for spam and malicious emails, including an inbound spam filter and outbound filtering with data loss prevention. SpamTitan performs reputation checks of the sender’s domain and email account, recipient verification, anti-spoofing checks, and alias recognition, and allows geoblocking to prevent the delivery of emails from certain locations (overseas, for instance).

SpamTitan also incorporates extensive content filtering mechanisms, including rewriting URLs to identify the true destination, URL checks to identify malicious content, anti-phishing measures including machine learning algorithms to detect suspicious content that deviates from the standard emails typically received, Bayesian analysis to identify spam and phishing, OLE detection, dual antivirus engines, and email sandboxing. Sandboxing is key to blocking malware threats, including previously unseen malware. With SpamTitan in place, the vast majority of threats will not arrive in inboxes. In recent independent tests, SpamTitan had a 99.99% spam detection rate, a 99.98% phishing detection rate, and a 100% malware detection rate, with zero false positives.

TitanHQ also offers a comprehensive security awareness training platform called SafeTitan. SafeTitan makes it easy for businesses to create and automate security awareness training programs for the workforce, and tailor programs for different departments and user groups. The content is fun and engaging and is delivered in modules of more than 10 minutes, which makes security awareness training easy to fit into busy workflows. SafeTitan also includes a phishing simulator for assessing the effectiveness of training and for giving employees practice at identifying phishing attempts, including the types of phishing attempts mentioned in this article that often fool employees.

SpamTitan and SafeTitan, like all TitanHQ solutions, are easy to implement, use, and maintain, and are available on a free trial. For advice on improving cybersecurity at your business and for further information on TitanHQ solutions, call the team today and take the first step toward improving your security posture.

AI Tools Increasingly Used for BEC/VEC Attacks

by G Hunt | August 27, 2024 | Phishing & Email Spam, Security Awareness

Business email compromise (BEC) and vendor email compromise (VEC) attacks can result in huge financial losses that can prove catastrophic for businesses, and these attacks are being conducted with increasing regularity.

BEC and VEC attacks have their roots in phishing and often involve phishing as the first stage of the attack. These attacks involve impersonation of a trusted person through spoofed or compromised email accounts. The attacker then tricks the targeted individual into disclosing sensitive information or making a fraudulent wire transfer. In the case of the latter, the losses can be considerable. A company employee at Orion, a Luxembourg carbon black supplier, resulted in fraudulent transfers of $60 million. The employee was tricked into believing he was conversing with a trusted vendor and made multiple fraudulent transfers to the attacker’s account.

BEC and VEC attacks are among the most difficult email threats to detect, as they often use legitimate, trusted email accounts so the recipient of the email is unaware that they are conversing with a scammer. Since the attacker often has access to emails, they will be aware of confidential information that no other individual other than the genuine account holder should know. The attacker can also check past emails between the account holder and the victim and can mimic the writing style of the account holder. These attacks can be almost impossible for humans to distinguish from genuine communications. Scammers often reply to existing email threads, which makes these scams even more believable.

BEC/VEC scammers are increasingly turning to AI tools to improve their attacks and AI tools make these scams even harder for humans and email security solutions to identify. AI tools can be fed past emails between two individuals and told to create a new email by mimicking the writing style, resulting in perfect emails that could fool even the most security-aware individual.

Some of the most convincing VEC attacks involve the use of compromised email accounts. The attacker gains access to the account through phishing or stolen credentials and searches through the account for information of interest that can be used in the scam. By searching through sent and stored emails, they can identify the vendor’s clients and identify targets. They are then sent payment requests for fake invoices, or requests are made to change the bank account information for genuine upcoming payments.

Due to the difficulty of identifying these threats, a variety of measures should be implemented to improve defenses, including administrative and technical controls, as well as employee training. In order to beat AI tools, network defenders need to adopt AI themselves, and should implement a spam filter with AI and machine learning capabilities, such as the SpamTitan cloud-based spam filtering service.

SpamTitan analyzes the genuine emails received by the company to create a baseline against which other emails can be measured. Through machine learning, Bayesian analysis, and other content checks, SpamTitan is able to identify the signs of BEC/VEC and alert end users when emails deviate from the norm. An anti-phishing solution is also strongly recommended to protect accounts against initial compromise and to raise awareness of potential threats. PhishTitan from TitanHQ incorporates cutting-edge threat detection with email banners warning about external emails and other threats and allows IT teams to rapidly remediate any attacks in progress.

Security awareness training is essential for raising awareness of the threat of BEC and VEC attacks. Since these scams target executives, IT, and HR staff, training for those users is vital. They should be made aware of the threat, taught how to identify these scams, and the actions to take when a potentially malicious message is received. With the SafeTitan security awareness training program it is easy to create training courses and tailor the content to cover threats each user group is likely to encounter to ensure the training is laser-focused on the most pertinent threats.

While spam email filtering and security awareness training are the most important measures to implement, it is also important to strengthen defenses against phishing through the adoption of multi-factor authentication on all email accounts, to prevent initial compromise. Administrative controls should also be considered, such as requiring employees to verify any high-risk actions, such as changes to bank accounts or payment methods, and maintaining a contact list of verified contact information to allow phone verification of any high-risk change. This two-step verification method can protect against all BEC/VEC attacks and prevent fraudulent payments.

New SpamTitan Release Improves Protection Against Advanced Phishing and Malware Threats

by G Hunt | August 27, 2024 | Industry News

TitanHQ has upgraded its award-winning SpamTitan email security solution, with the latest release including several enhancements to improve protection against malware, phishing, and other advanced threats. The latest release – version 9 – of the flagship email security solution is named SpamTitan Skellig, which includes major enhancements to the anti-spam engine at the core of the solution to improve malware detection and new phishing enhancements to protect against ever-evolving sophisticated threats.

SpamTitan is a leading cloud-based anti-spam service that has been shown in recent independent tests to provide exceptional protection against spam, phishing emails, and malware. The hosted spam filter includes a next-gen email sandbox, up-to-the-minute threat intelligence feed, AI and machine learning algorithms, twin antivirus engines, and more. In June 2024, Virus Bulletin put the new version of SpamTitan to the test and gave it VBSpam+ certification, with the solution achieving the second-highest final score in the test of 12 leading email security solutions. SpamTitan successfully blocked all malware samples, only missed one phishing email, and did

not generate any false positives. SpamTitan had a malware catch rate of 100%, a phishing catch rate of 99.99%, a spam catch rate of 99.98%, and was given an overall score of 99.984%.

The update to SpamTitan Skellig will ensure that users continue to have best-in-class protection against email threats but there is more to the update than protecting against threats. SpamTitan has long been popular with end users due to the ease of use of the solution, which is why users consistently give the solution 5-star reviews. The latest release includes a brand new UI that is even more intuitive with improved navigation and better administrative functions across the board and makes it easier to onboard new users.

The upgraded version is available to all new users and current users can upgrade and get better protection at no additional cost for the upgrade and no change to the subscription price, with full assistance provided with upgrading if required. You can find out more about migrating to the new version here.

Microsoft 365 Flaw Confirms Need for Layered Phishing Protections for M365

by G Hunt | August 19, 2024 | Uncategorized

The latest figures from Microsoft indicate that in 2024, around 1 million businesses worldwide are using Microsoft 365, and in the United States alone there are around 1 million users of its Office suite. That makes Microsoft 365 a big target for cybercriminals, and phishing is the main way that M365 users are targeted. Microsoft includes cybersecurity protections for its customers that can block phishing emails and malware, and those protections do a reasonable job of blocking malicious emails; however, threats do bypass defenses and reach end users, which is why many businesses choose to augment Microsoft's protections with third-party anti-phishing and anti-malware solutions, and now there is another good reason to bolster protection.

Recent research has uncovered a flaw in Microsoft's anti-phishing measures that allows cybercriminals to bypass its email safety alerts. Microsoft's First Contact Safety Tip generates these warnings when a user receives an email from an unfamiliar email address to warn them that the email may be malicious. The email will include the message "You don't often get emails from xxx@xxx.com. Learn why this is important." That message warns the user to take extra care and if it is not shown in the email the user may assume that the message is legitimate.

That warning message is added to the body of the HTML email and the problem with that approach is it is possible to manipulate the message by embedding Cascading Style Sheets (CSS), which is what researchers at Certitude discovered. They demonstrated that by manipulating the CSS within the HTML of the email, they were able to hide that warning, They did that by hiding the anchor tags (<a>) so the link is not displayed, changing the font color to white, and forcing the email to have a white background, ensuring that the text is not displayed since it is also in white. While the warning is still included in the email this trick renders it invisible. They also showed that it is possible to spoof Microsoft's encrypted and signed icons to make the email appear secure.

Microsoft has confirmed that the finding is valid but has chosen not to address the problem at this time. Microsoft has instead marked the issue for potential resolution through future product updates but there have been no known cases of this tactic being used in the wild and the issue was deemed to be sufficiently severe to qualify for immediate servicing.

This issue serves as a reminder about M365 cybersecurity. Microsoft produces some excellent products that are invaluable to businesses, but Microsoft is not a cybersecurity vendor and while protections have been added, they can be circumvented. Microsoft 365's EOP and Defender solutions do a good job at blocking most threats, but malicious emails do get through to inboxes where they can be opened by end users. The Microsoft 365 spam filter only provides an average level of protection against email threats.

TitanHQ has developed cybersecurity solutions to address M365 security gaps and provide greater protection for Microsoft 365 users through the SpamTitan spam filter for M365 and PhishTitan anti-phishing solution, both of which integrate seamlessly with Microsoft 365 and add important extra layers of protection against phishing, scam emails, and malware.

The engine that powers the SpamTItan and PhishTitan solutions has been independently tested and confirmed to provide superior protection through advanced features designed to catch more malicious emails. Those measures include a powerful next-generation email sandbox for protecting against advanced email attacks. When emails pass initial checks and scans using twin antivirus engines, they are sent to the sandbox for deep inspection, which allows malware to be identified from its behavior rather than a signature. These solutions include AI and machine learning protection, where malicious emails can be identified based on how they deviate from the normal emails received by a business, improving protection against zero-day threats – phishing and business email compromise emails that have not been seen before.

The PhishTitan solution has been developed specifically for Microsoft 365 to provide unmatched protection against phishing threats. PhishTitan displays banner notifications in emails to warn end users about suspicious content, which will provide protection should Microsoft's First Contact Safety Tip be hidden. Links in emails are rewritten to display their true destination, and the solution makes it quick and easy for security teams to remediate phishing threats throughout the entire email system.

The engine that powers these solutions has recently been shown to beat leading email security solutions such as Mimecast for catch rate, malware catch rate, and has far lower false positives. In the June Virus Bulletin Test, TitanHQ had a 99.99% phishing catch rate, a spam catch rate of 99.98%, a malware catch rate of 100%, and zero false positives. PhishTitan catches 20 unique and sophisticated threats per 80,000 emails received that Microsoft

365 misses. Give TitanHQ a call today to find out more about these solutions and how adding extra layers of protection can strengthen your business's security posture.

$60 Million Lost in Single Business Email Compromise Scam

by G Hunt | August 15, 2024 | Phishing & Email Spam, Security Awareness

Business Email Compromise (BEC) has long been one of the costliest types of cybercrime. According to the latest data from the Federal Bureau of Investigation (FBI) Internet Crime Compliant Center (IC3), almost 21,500 complaints were received about BEC attacks in 2023 resulting in adjusted losses of more than $2.9 billion. Between October 2013 and December 202, more than $50 billion was lost to BEC scams domestically and internationally.

What is Business Email Compromise?

BEC, also known as email account compromise (EAC), is a sophisticated scam that involves sending emails to individuals that appear to have come from a trusted source and making a legitimate-sounding request, which is typically a change to bank account details for an upcoming payment or payment of a fake invoice.

One such scam targets homebuyers, with the attacker impersonating the title company and sending details for a wire transfer for a down payment for a house purchase. Businesses are commonly targeted and asked to wire money for an upcoming payment to a different bank account. While the scammer is usually based overseas, the bank account may be at a bank in the victim's home country. When the funds are transferred by the victim they are immediately transferred overseas or withdrawn, making it difficult for the funds to be recovered.

BEC attacks often start with phishing emails. The scammers use phishing to gain access to an employee's email account, then the account is used to send phishing emails internally. The goal is to compromise the account of an executive such as the CEO or CFO. That account can then be used for the BEC part of the scam. Alternatively, vendors are targeted, such as construction companies, and their accounts are used for BEC attacks on their customers.

Once a suitable email account has been compromised, the scammers search through previous emails in the account to find potential targets – the company's customers in the case of a vendor account or individuals responsible for making wire transfers in the case of a CEO's account. The attackers study previous communications between individuals to learn the writing style of the account holder, and then craft their messages impersonating the genuine account owner. AI tools may also be used for this part of the scam or even researching targets. Alternatively, email accounts and websites may be spoofed, using slight variations of legitimate email addresses and domains. The information needed to conduct the scam may be gleaned from public sources or stolen via malware infections.

From here, a single request may be sent or a conversation may ensue over several emails to build trust before the request is made. Considerable time and effort is put into these scams because the effort is worth it for the scammers. The losses to these scams can be huge. Fraudulent wire transfers are often for tens of thousands of dollars or more, and with two recent scams, the losses have been immense.

Tens of Millions Fraudulently Obtained in BEC Scams

INTERPOL recently reported that it had successfully recovered more than $40 million stolen in a single BEC attack. The scammers targeted a commodities firm in Singapore, impersonating one of the company's suppliers. In July, an email was received that had apparently been sent by the supplier requesting a pending payment be sent to a new bank account, in this case, the account was based in Timor Leste. In this scam, the email was sent from an account that differed slightly from the supplier's legitimate email address. That difference was not identified and the bank account details were changed. A payment of $42.3 million was made to the account, and the transfer was only determined to be fraudulent when the supplier queried why the payment had not been received. INTERPOL was able to assist with the recovery of $39 million, and seven arrests were made which also involved the recovery of a further $2 million.

There has since been an even bigger scam and the victim was not so fortunate. The chemical manufacturing company Orion reported falling victim to a BEC attack that resulted in a $60 million loss. The Luxembourg firm told the U.S. Securities and Exchange Commission (SEC) that a non-executive employee was tricked into transferring the funds to multiple third-party accounts. So far, that loss has not been recovered.

How to Reduce Risk And Defeat BEC Attacks

Defending against BEC attacks can be a challenge, as legitimate email accounts are often used and the scammers are expert impersonators. The use of AI tools makes these scams even more difficult to identify. Defending against BEC attacks requires a defense-in-depth approach to prevent malicious emails from being delivered and prepare the workforce by improving awareness of the threats.

Security awareness training is vital. All members of the workforce should receive training and be made aware of BEC scams (and other cybersecurity threats). Training should cover the basics of these scams, such as why they are conducted and the attackers' aims, as well as the red flags to look for. Phishing simulations can be highly beneficial, as BEC scams can be simulated to put training to the test and give individual practice at identifying these scams. TitanHQ's SafeTitan platform includes BEC training material and a phishing simulator and makes it easy for businesses to improve their human defenses against BEC attacks.

Policies and procedures should be developed and implemented to reduce risk. For instance, it should be company policy for any requested change to banking credentials to be reviewed by a supervisor, and for any requested bank account changes by vendors to require verification by phone, using previously verified contact information.

It is vital to implement technical security measures to prevent email accounts from being compromised, malware from being installed, and to identify and block BEC emails. Traditional anti-spam software often fails to detect these sophisticated threats. A standard anti-spam appliance will perform a range of checks on the sender's reputation and may be able to detect and block spoofed emails, but generally not emails sent from legitimate compromised accounts. Traditional anti-spam and antivirus solutions can detect known malware, but not novel malware threats.

What is needed is a next-generation hosted anti-spam service with machine learning and AI capabilities that can learn about the standard emails sent and received by a company or individual and determine when emails deviate

from the norm and flag them as suspicious. AI-based protection is needed to defeat cybercriminals ‘ use of AI tools. The spam filtering service should also include email sandboxing in addition to standard anti-virus protection to identify and block novel malware threats, to prevent the malware infections that are used to gather information to support BEC attacks. SpamTitan from TitanHQ has all these features and more, with recent independent tests confirming the solution provides exceptional protection against phishing, spam, and sophisticated threats such as BEC attacks.

The most important thing to do is to take proactive steps to improve your defenses. Doing nothing could see your business featured in the next set of FBI statistics. Give the TitanHQ team a call today to discuss the best defenses for your business and find out more about how TitanHQ can help block BEC attacks and other cyber threats.

Training, Automation, AI, and Machine Learning Key to Reducing Data Breach Costs

by G Hunt | July 31, 2024 | Network Security

Each year, IBM conducts a study of data breaches to determine how much these incidents are costing businesses, the main factors that contribute to that cost, and how attackers are gaining access to their victims’ networks. Aside from 2020, data breach costs have continued to increase annually, and this year is no exception. The average cost of a data breach has risen from $3.86 million in 2018 to $4.88 million in 2024 and has increased by 10% since last year. The highest costs were incurred at critical infrastructure entities, especially healthcare organizations. Breaches at the latter were the costliest at an average of $9.77 million per incident.

The report is based on 3,556 interviews with individuals at 604 organizations who had knowledge about data breaches at their respective organizations. The data breaches included in the report involved between 2,100 and 113,000 compromised records and occurred between March 2023 and February 2024. The calculations include direct costs such as the breach response, ransom paid, forensic analysis, and regulatory fines, as well as indirect expenses such as in-house investigations, loss of business, and loss of customers.

This year’s *Cost of a Data Breach Report* revealed the high cost of breaches stemming from phishing, business email compromise, social engineering, and stolen credentials, which are the costliest incidents to resolve. Breaches stemming from stolen credentials and phishing were the costliest root cause, as was the case in 2023. Compromised credentials were the leading attack vector and were behind 16% of breaches, with phishing the next most common behind 15% of breaches. In terms of cost, phishing attacks cost an average of $4.88 million and compromised credentials cost $4.81 million. Business email compromise attacks were also costly at an average of $4.88 million with social engineering incidents costing an average of $4.77 million.

The report dives into the factors that contribute to the cost of a breach and the main areas where businesses have been able to reduce costs. The main factors that contributed to the cost of a breach were security system complexity, a security skills shortage, and third-party breaches, which are difficult things to address. Businesses have been able to reduce breach costs by implementing a number of measures, and the two biggest factors were employee training and AI/machine learning insights, with one constant identified being the use of AI and automation in security.

Employee training was determined to reduce the average breach cost by $258,629, with the most important aspect of training related to detecting and stopping phishing attacks. If a business is targeted in a phishing campaign, it may not be possible to prevent all employees from being fooled by the campaign, but through regular training and phishing simulations, the severity of the incident can be greatly reduced. For instance, a recent phishing attack on a U.S. healthcare organization resulted in more than 50 email accounts being compromised. More effective training could have prevented many of those employees from being tricked, greatly reducing the severity of the attack and the cost of remediation.

AI and machine learning insights were determined to reduce the average breach cost by $258,538, a close second in terms of cost reduction. Cybercriminals are leveraging AI in their attacks, especially for phishing and social engineering attacks. Network defenders need to leverage AI and machine learning tools to help them defend against these attacks and identify phishing, social engineering, and BEC threats, which are becoming much harder for humans to spot. Automation is key, especially due to the cybersecurity skills shortage – one of the leading factors that increases breach costs. Network defenders are overworked, and automation is key to reducing their workload, especially since it is difficult to find and retain skilled cybersecurity staff.

At TitanHQ, we understand the importance of staff training, and the benefits of AI, machine learning, and automation and offer businesses an easy way to implement these and better protect themselves from cyberattacks, remediate incidents quickly and efficiently, and ensure that their workforce is well trained and aware of cyber threats and how to avoid them. Security awareness training is provided through the SafeTitan platform, which includes an extensive library of engaging training content to teach security best practices, raise awareness of cyber threats, and teach employees how to recognize and avoid threats including phishing, social engineering, and business email compromise.

The content is constantly refreshed to account for changing work practices, technology, and the latest tactics, techniques, and procedures being used by cybercriminals. The phishing simulator includes hundreds of templates taken from real-world phishing attempts to reinforce training and identify employees who fall for phishing attempts. It is quick and easy to create training courses and phishing simulations, and importantly, to automate them to run continuously throughout the year. The platform also automatically delivers training modules to employees in response to mistakes such as phishing simulation failures, to ensure training is delivered in real-time when it is needed the most and likely to have the greatest impact.

TitanHQ offers two cutting-edge products to protect against email-based attacks, especially phishing and social engineering attempts. SpamTitan is a cloud-based anti-spam service (or can be provided as a gateway spam filter) that incorporates exceptional malware protection, email sandboxing, AI, and machine learning algorithms to identify and quarantine sophisticated threats, including novel threats that have not been seen before. In recent independent tests, the machine learning algorithms and other threat detection features achieved a detection rate of over 99.99%.

PhishTitan incorporates the same AI and machine learning capabilities to identify and block more threats in Office 365 environments. PhishTitan layers extra protection on top of Microsoft 365's EOP and Defender provides best-in-class phishing protection. PhishTitan is also a remediation solution for automating the response to phishing threats to reduce the burden on IT staff, including instant inbox threat removal of emails containing malicious URLs and tenant-wide remediation with robust cross-tenant features for detection and response.

With these solutions, businesses can improve protection, prevent data breaches, and greatly reduce costs while easing the burden on their IT staff. They are also easy to implement and use, as we understand that IT staff don't need any more management headaches. For more information, give the TitanHQ team a call to discuss your requirements, find out more about the products, and arrange a product demonstration. All three products are also available in a free trial to allow you to put them to the test and see the difference they make.

Massive Phishing Campaign Defeats SPF and DKIM by Leveraging Proofpoint Misconfiguration

by G Hunt | July 31, 2024 | Phishing & Email Spam

A massive phishing campaign that involved around 3 million emails a day was made possible due to a misconfiguration in Proofpoint's email servers. The vulnerability was exploited to get the emails DomainKeys Identified Mail (DKIM) signed and approved by SPF, thereby ensuring the emails were delivered to inboxes.

Researchers at Guardio identified the campaign, which ran from January 2024 to June 2024 and at its peak involved sending around 14 million emails a day. The purpose of the campaign was to steal credit card numbers and set up regular credit card payments. The emails impersonated well-known brands such as Nike, Disney, Coca-Cola, and IBM. As is common in phishing attempts, the headers of the emails were spoofed to make it appear that the email had been sent by a genuine company. The majority of spam filters would be able to detect this spoofing and block the emails because they use Sender Policy Framework (SPF) and DKIM, specifically to detect and prevent spoofing.

Emails must be sent from approved servers to pass SPF checks and they must be authenticated using the DKIM encryption key for the domain. With DKIM, public-key cryptography is used to sign an email with a private key when it leaves the sender's server, and the recipient server uses the public key to verify the source of the message. If the from filed matches the DKIM check is passed and the email is determined to be authentic and will be delivered. If not, the email will identified as spam and will be blocked. In this campaign the emails were all properly signed and authenticated, ensuring that they would be delivered.

For an email that impersonated Nike, a spoofed email address would be used with the nike.com domain, which thanks to passing the SPF and DKIM checks, would be verified by the recipient as having been authenticated. The recipient may be fooled that the email has come from the genuine company domain, and since the emails themselves contained that company's branding and provided a plausible reason for taking action, the user may click the link in the email.

As with most phishing emails, there is urgency. Action must be taken quickly to avoid negative consequences, such as an impending charge, notification about the closure of an account, or another pressing matter. If the link is clicked, the user will be directed to a phishing site that also spoofs the brand and they are asked to provide their credit card details. Alternatively, they are offered a too-good-to-be-true offer, and by paying they also enroll in an ongoing subscription involving sizeable monthly charges.

The way that the attackers got around the checks was to send the emails from an SMTP server on a virtual server under their control and to route them through a genuine Office 365 account on an Online Exchange server, then through a domain-specific Proofpoint server which sent the email on to the intended recipient. Since the

Proofpoint customers being spoofed had authorized the Proofpoint service to send emails on their behalf as an allowed email sender, the attackers only had to find a way to send spoofed emails through the Proofpoint relay. Due to a misconfiguration that allowed Microsoft Office 365 accounts to easily interact with its relay servers, they were able to do just that, pass SPF and DKIM checks, and make their fake emails appear to be clean.

They obtained the MX record for the company being spoofed by querying the domain's public DNS, then routed the email through the correct Proofpoint host that is used to process email for that domain. Since the Proofpoint server was tricked into believing that the emails had come from the genuine domains of its customers – such as Nike and Disney – the emails were then forwarded to the intended recipients rather than being quarantined.

Spammers are constantly developing new methods of defeating the best email security solutions and while email security products can usually block spam and malicious emails, some will be delivered to recipients. This is why it is important to have layered defenses in place to protect against all phases of the attack. For instance, in this attack, spam filters were bypassed, but other measures could detect and block this attack. For instance, a web filter can be used to prevent a user from visiting a phishing website linked in an email, and security awareness training should be conducted to teach employees how to identify the signs of phishing, to check the domain of any website linked in an email, and to also check the domain when they arrive on any website.

Microsoft Forms Used in Phishing Campaign Targeting M365 Credentials

by G Hunt | July 31, 2024 | Phishing & Email Spam

Microsoft credentials are being targeted in phishing campaigns that abuse Microsoft Forms. Microsoft Forms is a feature of Microsoft 365 that is commonly used for creating quizzes and surveys. Microsoft Forms has been used in the past for phishing campaigns, and Microsoft has implemented phishing protection measures to prevent abuse, but these campaigns show that those measures are not always effective.

To increase the probability of the phishing emails being delivered and the recipients responding, threat actors use compromised email accounts for the campaigns. If a business email account can be compromised in a phishing attack, it can be used to send phishing emails internally. Vendor email accounts are often targeted and used to conduct attacks on their customers. The emails are likely to be delivered as they come from a trusted account, which may even be whitelisted on email security solutions to ensure that their messages are delivered.

If the recipient clicks the link in the email they are directed to a Microsoft Form, which has an embedded link that the user is instructed to click. If the link is clicked, the user is directed to a phishing page where they are asked to enter their Microsoft 365 credentials. If the credentials are entered, they are captured by the attacker and are used to access their account.

The initial contact includes messages with a variety of lures, including fake delivery failure notifications, requests to change passwords, and notifications about shared documents. When the user lands on the form, they are told to click a link and fill in a questionnaire, that link then sends the user to a phishing page that appears to be a genuine login page for Microsoft 365 or another company, depending on which credentials are being targeted.

The attackers make their campaign more realistic by using company logos in the phishing emails and familiar favicons in the browser tab on the fake web pages. Since Microsoft Forms is used in this campaign, the URL

provided in the phishing emails has the format https://forms.office[dot]com, as the forms are on a genuine Microsoft Forms domain. Not only does that help to trick the user into thinking the request is genuine, but it also makes it much harder for email security solutions to determine that the email is not legitimate as the forms.office[dot]com is generally trusted as it has a high reputation score.

When these phishing campaigns are detected, Microsoft takes prompt action to block these scams. Each form has a 'report abuse' button, so if the scams are identified by users, Microsoft will be notified and can take action to shut it down. The problem is that these emails are being sent in huge numbers and there is a considerable window of opportunity for the attacks. Further, if the attacker's campaign is detected, they can just set up different web pages and forms and continue.

These phishing campaigns involve two phases, the first phase involves compromising email accounts to send the initial phishing emails. An advanced email security solution with sandboxing, URL rewriting, and AI-based detection capabilities will help to block this first phase of the attack. Advanced anti-phishing solutions for Office 365 can reduce the number of phishing emails that land in inboxes, even when sent from trusted email accounts. Banner warnings in emails will help to alert users to potential phishing emails; however, users need to be vigilant as it may be up to them to spot and report the phishing attempt. That means security awareness training should be provided to raise awareness of these types of phishing attempts.

Security awareness training should also incorporate phishing simulations, and it is recommended to create simulations of phishing attempts using Microsoft Forms. If users fall for the fake Microsoft Forms phishing attempts, they can be provided with further training and told how they could have identified the scam. If another Microsoft Forms phishing attempt is received, they are more likely to be able to identify it for what it is.

TitanHQ can help businesses improve their defenses against phishing through the TitanHQ cybersecurity suite, which includes SpamTitan cloud-based anti-spam service, the PhishTitan anti-phishing solution, and the SafeTitan security awareness and phishing simulation platform. SpamTitan and PhishTitan have exceptionally high detection rates with a low false positive rate, and SafeTitan is the only behavior-driven security awareness training platform that delivers training in real-time in response to employee mistakes. Give the TitanHQ team a call today for more information about these products, you can book a product demonstration to find out more, and all solutions are available on a free trial.

Don't Put Up with Substandard Phishing Protection for M365!

by G Hunt | July 29, 2024 | Phishing & Email Spam

Businesses that rely on Microsoft Defender for detecting malware and phishing emails may not be as well protected as they think. While Defender performs a reasonable job at blocking malware, spam, and phishing emails, it lacks the high detection levels of many third-party anti-phishing solutions.

Take malware for example. A study conducted in 2022 by AV-Comparatives found Defender only had a 60.3% offline detection rate. Fast forward to Q2, 2024, and TitanHQ's email security suite was put to the test alongside 12 other email security solutions by Virus Bulletin. In the independent tests, TitanHQ had a malware catch rate of 100%.

In the same round of testing, TitanHQ's spam filter for Office 365 and the email security suite had a spam catch rate of over 99.98%, a phishing email catch rate of 99.99%, and was given an overall final score of 99.984, the second highest in the tests. It is possible to configure an email solution to provide maximum protection; however, that will be at the expense of an elevated number of false positives – genuine emails that are inadvertently marked as potentially suspicious and are quarantined until they are released by an administrator. In the tests, TitanHQ had a 0.00% false positive rate, with no genuine emails misclassified.

Another issue with Microsoft Defender is the exception list, which contains locations such as files, folders, and processes that are never scanned. These are used to ensure that legitimate apps are not scanned, to prevent them from being misclassified as malware. The problem is that the exception list lacks security protections, which means it can be accessed internally by all users. Should a device be compromised, a threat actor could access the exceptions list, identify folders and files that are not scanned, and use those locations to hide malware.

Given the increasingly dangerous threat environment and the high costs of a cyberattack and data breach, businesses need to ensure they are well-defended, which is why many businesses are choosing to protect their Microsoft 365 environments with TitanHQ's PhishTitan anti-phishing solution.

PhishTitan is a cloud-based, AI-driven solution for Microsoft 365 that integrates seamlessly into M365 to increase protection from sophisticated phishing attacks. Rather than replacing Microsoft's EOP and Defender protections, PhishTitan augments them and adds next-generation phishing protection, not only ensuring that more threats are blocked but also giving users easy-to-use remediation capabilities.

PhishTitan adds advanced threat detection capabilities through machine learning and LLM to identify the zero-day and emerging threats that are missed by Defender. PhishTitan provides real-time protection against phishing links in emails in addition to checks performed when the email is received. URLs are rewritten for Link Lock protection with all links reassessed at the point a user clicks to ensure that URLs that have been made malicious after delivery are detected and blocked. If the link is detected as malicious, access to that URL will be prevented.

PhishTitan also adds banner notifications to emails to alert users to unsafe content and emails from external sources, and the auto-remediation feature allows all threats to be instantly removed from the entire mail system, with robust cross-tenant features for detection and response for MSPs.

PhishTitan has also been developed to be quick to set up and configure. There is no need to change MX records, setup typically takes less than 10 minutes, and the solution is incredibly easy to manage. Why put up with inferior threat detection and complex interfaces, when you can improve the Office 365 phishing protection with an easy-to-use anti-phishing solution

Don't take our word for it though. Take advantage of the free trial of PhishTitan to see for yourself. Product demonstrations can also be arranged on request.

ZeroFont Phishing Scam Targets Microsoft 365 Users

by G Hunt | July 27, 2024 | Phishing & Email Spam

A ZeroFont phishing campaign is being conducted that targets Microsoft 365 users. Rather than using the ZeroFont technique to hide malicious content from anti-spam software, this method aims to trick end users into

thinking the email is genuine and safe.

The ZeroFont phishing technique was first identified in phishing attempts around five years ago, so it is not a new technique; however, this version uses a novel approach. When an email is sent to a business user, before that email is delivered it will be subject to various checks by the anti-spam server. The business's anti-spam solution will perform reputation checks, scan the email for malware, and analyze the content of the email to search for signs of spam or phishing. Only if those checks are passed will the message be delivered to the end user. ZeroFont is a technique for hiding certain words from email security solutions to ensure that the messages are not flagged as spam and are delivered.

According to Check Point, Microsoft is the most commonly impersonated brand in phishing emails. If a threat actor impersonates Microsoft, they obviously cannot send the email from the Microsoft domain as they do not have access. Spam filters will check to make sure that the domain from which the email is sent matches the signature, and if there is no match, that is a strong signal that the email is not genuine. With ZeroFont, the signature used would only display Microsoft to the end user, and the spam filter is presented with a nonsensical string of text. The user would not see that text as the padding text around the word Microsoft is set to a font size of zero, which means the text is machine-readable but cannot be seen by the user.

A recent campaign uses the ZeroFont techniques but with a twist. In this campaign, the aim is not to trick a spam filter but to instead trick Outlook users. In Outlook, it is possible to configure the mail client with a listing view option, which will show the user the first lines of text of an email. The problem for phishers is getting Outlook users to engage with the messages, which means the messages must be sufficiently compelling so as not to be deleted without opening them. This is especially important if the sender of the email is not known to the recipient.

The email was detected by Jan Kopriva, who noticed that ZeroFont was used to make the message appear trustworthy by displaying text indicating the message had been scanned and secured by the email security solution, rather than showing the first lines of visible content of the message. This was achieved by using a zero font size for some of the text. The threat actor knew that the first lines of the emails are displayed by the mail client in the listing view, regardless of the font size, which means if the font is set to zero, the text will be displayed in the listing view but will not be visible to the user in the message body when the email is opened.

The email used a fake job offer as a lure and asked the user to reply with their personal information: Full name, address, phone number, and personal email, and impersonated the SANS Technology Institute. The full purpose of the phishing attempt is not known. There were no malicious links in the email and no malware attached so the email would likely pass through spam filters. If a response is received, the personal information could be used for a spear phishing attempt on the user's personal email account, which is less likely to have robust spam filtering in place, or for a voice phishing attempt, as we have seen in many callback phishing campaigns.

Security awareness training programs train employees to look for signs of phishing and other malicious communications, and they are often heavily focused on embedded links in emails and attachments. Emails such as this and callback phishing attempts lack the standard malicious content and as such, end users may not identify them as phishing attempts. It is important to incorporate phishing emails such as this in security awareness training programs to raise awareness of the threat.

That is easy with SafeTitan from TitanHQ, as is conducting phishing simulations with these atypical message formats. SafeTitan includes a huge library of security awareness training content, and the phishing simulator includes thousands of phishing templates from real-world phishing attempts. It is easy for businesses to create and automate comprehensive security awareness training programs for the workforce and provide training on how to identify novel techniques such as this when they are identified, to ensure employees are kept up to date on the latest tactics, techniques, and procedures used by cybercriminals.

CrowdStrike Phishing and Malware Distribution Scams Mount Following Outage

by G Hunt | July 26, 2024 | Phishing & Email Spam

CrowdStrike has confirmed that a significant proportion of Windows devices that were rendered inoperable following a faulty update last Friday have now been restored to full functionality; however, businesses are still facing disruption and many scams have been identified by cybercriminals looking to take advantage.

One of those scams involves a fake recovery manual that is being pushed in phishing emails. The emails claim to provide a Recovery Tool that fixes the out-of-bounds memory read triggered by the update that caused Windows devices to crash and display the blue screen of death. The phishing emails include a document attachment named “New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows. docm.” The document is a copy of a Microsoft support bulletin, which claims that a new Microsoft Recovery Tool has been developed that automates recovery by deleting the CrowdStrike driver that is causing the crash. The user is prompted to enable content; however, doing so will allow a macro to run, which will download a malicious DLL, which launches the Daolpu stealer – an information stealer that collects and exfiltrates credentials, login information, and cookies stored in Chrome and Firefox.

Another campaign has been identified that capitalizes on the defective Falcon Sensor update. The spear phishing campaign targeted German firms and attempts to distribute a fake CrowdStrike Crash Reporter installer via a website that spoofs a legitimate German company. The website was registered a day after the CrowdStrike disruptions started. If the user attempts to download the installer by clicking the download button in the email, a ZIP archive will be delivered that includes a malicious InnoSetup installer. If executed, the user is shown a fake CrowdStrike branded installer. The installer is password-protected to prevent analysis and the final payload could not be determined.

Another campaign attempts to distribute Lumma information-stealing malware. The campaign uses the domain, crowdstrike-office365[.]com, and tricks the recipient into downloading a fake recovery tool to deal with the boot loop that prevents Windows devices from booting up. If the downloaded file is executed, it delivers a malware loader, which will, in turn, deliver the Lumma infostealer.

These are just three campaigns that use the CrowdStrike outage to deliver malware, all of which use email as the way to make contact with individuals affected by the outage. Many other campaigns are being conducted and a large number of CrowdStrike-themed domains have been registered since the problems started. Other malicious domains used in campaigns include the following, all of which should be blocked.

crowdstrike-helpdesk.com

crowdstrike.black

crowdstrikefix.zip

crowdstrikebluescreen.com

crashstrike.com

fix-crowdstrike-bsod.com

crowdstrike-falcon.online

crowdstrike-bsod.com

crowdstrikedoomsday.com

crowdstrikedown.site

crowdstrikefix.com

isitcrowdstrike.com

crowdstriketoken.com

crowdstrike0day.com

crowdstrikeoutage.com

These scams are likely to continue for some time, so it is important to remind employees of the high risk of malicious emails and warn them to exercise extreme caution with any emails received. Employees should be told to report any suspicious emails to their security team.

TitanHQ offers a range of cybersecurity solutions to block phishing and malware distribution campaigns, all of which are quick and easy to implement and can protect you in a matter of minutes. They include the WebTitan web filter for blocking access to known malicious websites, such as those detailed in this email; the PhishTitan anti-phishing solution for Office 365, and the SpamTitan corporate email filter for blocking phishing emails. The latter incorporates email sandboxing for blocking novel and obfuscated malware threats. TitanHQ also provides a comprehensive security awareness training platform and phishing simulator for improving your human defenses by raising awareness of cyber threats and providing timely training content on the latest tactics used by cybercriminals in targeted attacks on employees.

Give the TitanHQ team a call today for further information on improving your defenses, or take advantage of the free trial available with all TitanHQ products to get immediate protection.

Surge in Fake Websites and Phishing Related to CrowdStrike Windows Outage

by G Hunt | July 22, 2024 | Phishing & Email Spam

On July 19, 2024, Windows workstations and servers were disabled as a result of a bug in a software update for CrowdStrike Falcon Sensor. When the update was installed on Windows devices, it caused them to show the Blue Screen of Death or get stuck in a boot loop, rendering the devices unusable. Microsoft revealed that its telemetry showed 8.5 million Windows devices had been affected in around 78 minutes.

CrowdStrike Falcon platform is a cybersecurity solution that incorporates anti-virus protection, endpoint detection and response, threat intelligence, threat hunting, and security hygiene, and it is used by many large businesses around the world, including around half of Fortune 500 firms. The disruption caused by the update has been colossal. Airlines had to ground flights, airports were unable to check people in, healthcare providers were unable to access electronic patient records and had to cancel appointments and surgeries, financial institutions faced major disruption, and some media companies were unable to broadcast live television for hours. Even organizations that did not use the Falcon product were adversely affected if any of their vendors used the product. The incident has been called the worst-ever IT outage, with huge financial implications.

It did not take long for cybercriminals to take advantage of the chaos. Within hours, cybercriminals were registering fake websites impersonating CrowdStrike offering help fixing the problem, and domains were registered and used in phishing campaigns promising a rapid resolution of the problem. Given the huge financial impact of suddenly not having access to any Windows devices, there was a pressing need to get a rapid resolution but the fixes being touted by cybercriminals involved downloading fake updates and hotfixes that installed malware.

Those fake updates are being used to deliver a range of different malware types including malware loaders, remote access Trojans, data wipers, and information stealers, while the phishing campaigns direct users to websites where they are prompted to enter their credentials, which are captured and used to access accounts. Cybercriminals have been posing as tech specialists and independent researchers and have been using deepfake videos and voice calls to get users to unwittingly grant them access to their devices, disclose their passwords, or divulge other sensitive codes.

CrowdStrike has issued a fix and provided instructions for resolving the issue, but those instructions require each affected device to be manually fixed. The fix was rolled out rapidly, but CrowdStrike CEO George Kurtz said it will likely take some time for a full recovery for all affected users, creating a sizeable window of opportunity for threat actors. Due to the surge in criminal activity related to the outage, everyone should remain vigilant and verify the authenticity of any communications, including emails, text messages, and telephone calls, and only rely on trusted sources for guidance. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has reminded all organizations of the importance of having robust cybersecurity measures in place to protect their users, assets, and data, and to remind all employees to avoid opening suspicious emails or clicking on unverified links in emails.

It is important to have multiple layers of security protection to identify, detect, and avoid these attacks, including AI-driven phishing protection, web filtering to block access to malicious websites, anti-virus software to detect and neutralize malware, and security awareness training for employees. TitanHQ can help to secure your business in all of these areas and offers a cloud-based spam filtering service (SpamTitan) which includes email sandboxing and email antivirus filter, phishing protection for Office 365 (PhishTitan), and the SafeTitan security awareness training and phishing simulator.

Malicious Email Campaign Deliver a Malware Cluster Bomb of Up to 10 Viruses

by G Hunt | June 30, 2024 | Phishing & Email Spam

Many malware infections start with a malicious email that contains a file attachment with a malicious script that downloads malware if executed. One response to a single email is all it takes to infect the user's device with malware, which may be able to spread across the network or at least provide the threat actor with the foothold they need in the network for follow-on activities. There is a much worse scenario, however. Rather than a single user infecting the network with one malware variant, that single response to the malicious email results in multiple malware infections. One campaign has been identified that does just that. A malware cluster bomb is delivered that can infect the user's device with up to 10 different malware variants.

The campaign was identified by researchers at KrakenLabs and has been attributed to a threat actor known as Unfurling Hemlock. The campaign is being conducted globally with at least 10 countries known to have been attacked, although most of the victims have so far been located in the United States. The campaign has been running since at least February 2024 and uses two methods to deliver the malware variants – malicious emails and malware loaders installed by other threat groups. The threat actor has already distributed hundreds of thousands of malicious files in the 5 months since the operation is believed to have commenced.

In the email campaign conducted by Unfurling Hemlock, the victim is tricked into downloading a file called WExtract.exe which contains nested cabinet files, each containing a different malware variant. If the file is executed, the malware is extracted in sequence, and each malware variant is executed in reverse order, starting with the last malware variant to be extracted. Each malware cluster bomb has between four and seven stages, with some of those stages delivering multiple malware variants.

The malware variants delivered vary but they consist of information stealers, backdoors, malware loaders, and botnets. Information stealers include Redline Stealer, Mystic Stealer, and RisePro, and malware loaders including Amadey and SmokeLoader. Other malware variants are used to disable security solutions such as Windows Defender, help with obfuscation and hiding malware payloads, gathering system information, and reporting on the status of the malware infections.

It is not clear how the threat actor is using these malware infections. They could be delivering malware for other threat actors and selling the access, using the malware to harvest credentials to sell on the darkweb, conducting their own attacks using whatever malware variant serves their purpose, or a combination of the three. What the attack does ensure is maximum flexibility, as there are high levels of redundancy to ensure that if some of the malware variants are detected, some are likely to remain.

The delivery of multiple malware variants means this campaign could be highly damaging, but it also increases the chance of detection. While antivirus software is a must and may detect some of the malware variants, others are likely to go undetected. The key to blocking attacks is to prevent the initial phishing emails from reaching end users and to provide training to the workforce to help with the identification and avoidance of these malicious emails.

Many email security solutions rely on antivirus engines to detect malware but cybercriminals are skilled at bypassing these signature-based defenses. TitanHQ's SpamTitan anti-spam software, SpamTitan, uses dual

antivirus engines as part of the initial checks but also email sandboxing for behavioral analysis. Suspicious emails are sent to the sandbox where files are unpacked and their behavior is analyzed in depth. The behavioral analysis identifies malicious actions, resulting in the messages being quarantined for further analysis by the security team. SpamTitan also includes AI and machine-learning algorithms to check how messages deviate from the emails typically received and can identify new threats that have previously not been seen. SpamTitan is a highly effective Microsoft 365 spam filter and can be provided as a gateway spam filter or a cloud-based anti-spam service.

End user training is an important extra layer of security that helps eradicate bad security practices and teaches employees how to recognize and avoid malicious emails. Should a malicious bypass email security defenses, trained employees will be more likely to recognize and report the threat to the security team. Training data from SafeTitan, TitanHQ's security awareness training platform and phishing simulator, shows the training and phishing simulations can reduce susceptibility to email attacks by up to 80% when provided regularly throughout the year.

Give the TitanHQ sales team a call today for more information on these and other cybersecurity solutions to improve your defenses against the full range of cyber threats.

A Cost-Effective Way to Improve Office 365 Email Filtering

by G Hunt | June 29, 2024 | Phishing & Email Spam, Spam Advice

Around 40% of businesses use Office 365 for email, which includes Exchange Online Protection (EOP) with standard licenses for blocking spam and other email threats. While EOP will block a substantial amount of unwanted spam emails and malicious emails, the level of protection provided falls well below what many businesses need as too many threats pass through undetected.

Businesses can opt for a more expensive Business Premium license to improve Microsoft's spam filter for Office 365, as this license includes Defender for Office 365. Alternatively, businesses can pay for Defender as an add-on. While Defender improves the phishing detection rate, this security feature only adds a little extra protection to EOP, and many malicious emails still go undetected. The E5 license provides the greatest amount of protection but it is prohibitively expensive for many businesses, and even this license does not give you cutting-edge protection.

Fortunately, there is a way to improve Office 365 email filtering that will provide you with excellent protection against phishing, malware, spam, and other email threats without having to cover the cost of expensive licenses and add-ons. That solution is to use a third-party email security solution that augments the spam filter for Office 365 regardless of the license you have. Many businesses prefer to use a third-party solution rather than placing all of their trust in Microsoft – a company that has recently struggled with preventing hackers from compromising its own systems.

SpamTitan from TitanHQ is a cloud-based email security solution that integrates seamlessly with Office 365 to greatly increase protection against email threats such as phishing, business email compromise, malware, and data theft by insiders, and is easy to set up, configure, and manage.

There are several features of SpamTitan that are lacking in Microsoft's security solutions. In addition to performing reputation checks and blocking known malicious email addresses and domains, SpamTitan uses

predictive techniques for detecting spam and phishing emails, such as Bayesian analysis, machine learning, and heuristics. These features allow SpamTitan to detect and block zero-day phishing threats and business email compromise, which Microsoft struggles to detect and block.

SpamTitan performs extensive checks of embedded hyperlinks to combat phishing, including checks of Shortened URLs. Office 365 malware detection is greatly improved with dual antivirus engines for detecting known malware and email sandboxing. The sandboxing feature includes machine learning and behavioral analysis for the safe detonation of files in an isolated environment, and message sandboxing is vital for detecting and blocking the zero-day malware threats that EOP and Defender miss.

SpamTitan cloud-based email filtering is also an ideal choice for Managed Services Providers looking to provide their customers with more advanced email security, especially for small- and medium-sized clients unwilling to pay for E5 licenses. SpamTitan has been developed from the ground up to meet the needs of MSPs and manage email security with minimal management overhead.

TitanHQ can also MSPs additional protection against phishing with TitanHQ's new anti-phishing solution, PhishTitan. PhishTitan uses a large language model (LLM) and AI to analyze emails to identify phishing attempts. The solution incorporates multiple curated feeds to detect malicious URLs linked in phishing emails, adds banners to emails from external sources to warn end users about potential threats, and adds post-delivery remediation across multiple tenants allowing phishing emails to be instantly removed from the email system with a single click.

The best way to find out more about the full capabilities of SpamTitan and PhishTitan and how they work is to call the TitanHQ team. A product demonstration can be arranged and you can take advantage of a free trial to see for yourself the difference these solutions make and how they can significantly improve threat detection with Office 365.

New Campaigns Use Trojanized Software Downloaders to Distribute Dangerous Information Stealers

by G Hunt | June 28, 2024 | Phishing & Email Spam

Two new malware distribution campaigns have been detected that deliver dangerous information-stealing malware, both targeting individuals looking to download free and pirated software.

Trojaninized Cisco Webex Meetings App Delivers Malware Loader and Information Stealer

Another malware distribution campaign has been identified that is using trojanized installers for free and pirated software to deploy a malware loader called Hijack Loader, which in turn delivers an information stealer. In the attacks, the victim was tricked into downloading a trojanized version of the Cisco Webex Meetings App, a video streaming app. The user downloaded a password-protected archive (RAR) file, which contained a file called setup.exe. When the victim executed the file, DLL sideloading was used to launch the HijackLoader, which was injected into a Windows binary.

HijackLoader connects with its command-and-control server and downloads another binary, an information stealer called Vidar Stealer. The malware bypasses User Account Control (UAC), escalates privileges, and adds an exception to the Windows Defender exclusion list. Vidar Stealer is used to steal credentials from browsers and deliver additional malware payloads, including a cryptocurrency miner. This campaign primarily targets organizations in Latin America and the Asia Pacific region.

Google Ads Used to Target Mac Users and Deliver Poseidon Malware

An information stealer called Poseidon is being distributed via malicious Google Ads that claim to provide the popular Arc web browser. The campaign targets Mac users and delivers a trojanized version of the Arc browser installer. If the installer is launched, the user gets the browser but is also infected with the malware.

According to an analysis from Malwarebytes, the new information stealer has similar features to the notorious Atomic Stealer, including a file grabber, crypto wallet extractor, and the ability to steal passwords from password managers such as Bitwarden and KeepassXC, passwords stored in browsers, and browser histories. The targeting of password managers makes this malware particularly dangerous, potentially allowing the theft of all passwords. The researchers believe the malware has been set up as a rival to Atomic Stealer

How to Protect Your Business

Protecting against malware requires a defense-in-depth approach to security, where several different security solutions provide multiple overlapping layers of protection. These security measures should include the following:

Antivirus software – Antivirus software is a must. The software will be able to detect malware when it is downloaded onto a device or is executed. The malware is identified by its signature, which means that a particular malware variant must be known and its signature must be present in the malware definition list used by that software. Antivirus software will not detect novel malware variants without behavioral analysis of files.

Web filter – One of the best defenses against malware distributed via the internet is a web filter. The web filter blocks downloads of malicious files by preventing downloads of executable files from the Internet, blocking access to known malicious websites, and limiting the sites that users can visit on their corporate-owned devices. The main advantage of a web filter is the threat is dealt with before any files are downloaded from the Internet.

Security awareness training – Users should be warned about the risks of downloading software from the Internet, be taught how to identify the signs of phishing and malicious emails, and be trained on security best practices. The latter should include carefully checking the domain of the website offering software and making sure it is the official website of the software vendor or a reputable software distributor.

Email security solution – Malware is often delivered via email, usually via a malicious script in an attached file or via a linked web page. An email security solution needs to have antivirus capabilities – signature-based detection and behavioral analysis in an email sandbox. The former will detect known malware variants and email sandboxing is used to detect novel malware variants. Your email security solutions should also include AI-based detection, which can identify malicious messages based on how they differ from standard messages received by your business and perform comparisons with previous malware distribution campaigns.

While TitanHQ does not provide antivirus software, TitanHQ can help with web filtering (WebTitan), email security (SpamTitan), phishing protection (PhishTitan), and security awareness training (SafeTitan). For more information on improving your defenses against malware and TitanHQ's multi-award-winning cloud-based email security and internet security solutions for businesses and managed service providers, give the TitanHQ team a call today.

Oyster Backdoor Delivered Through Malvertising Campaign Offering Popular Software Solutions

by G Hunt | June 26, 2024 | Website Filtering

A malvertising campaign has been identified that targets users looking to download popular software such as Google Chrome and Microsoft Teams and delivers a backdoor malware called Oyster. The threat actor has registered lookalike domains that offer the software to download; however, the installer delivers the backdoor, with PowerShell used for persistence. After the malware is executed, the legitimate software is installed. Since the user gets the software they are expecting, they are unlikely to realize that their device has been infected.

The Oyster backdoor has been linked to the Russian threat group behind the infamous TrickBot Trojan. Once installed, the malware connects with its command-and-control server, gathers information about the host, and allows the threat actors to remotely execute code on the infected device. According to researchers at Rapid7 who identified the campaign, the threat actor has been observed delivering additional malware payloads on infected devices.

Malvertising is a common method of malware delivery that takes advantage of a lack of security awareness and attentiveness. Threat actors create adverts on legitimate ad networks for popular software solutions and pay to have their ads appear when users search for the software solutions they are impersonating. Just because an advert appears at the top of the search engine listings on Google or Bing it does not mean that the advert is legitimate. Clicking the link will direct the user to a site that is a carbon copy of the legitimate website that it spoofs, where they can download the software installer. These campaigns can be identified by the domain, which should be carefully checked to make sure it is the website of the official software provider.

Typosquatting is also commonly used, where threat actors register almost identical domains to the company they are impersonating. The domains usually have a transposed or missing letter. If the domain is not carefully checked, the user is unlikely to realize they are not on the official website. Threat actors use black hat search engine optimization techniques to get the websites to appear high up in the search engine listings.

By targeting software downloads, where the user is expecting to download an installer, the threat actor does not need to convince the user to execute the malicious file. If they fail to identify the scam before downloading the installer, their device is highly likely to be infected. Security awareness training should cover the methods used by threat actors to distribute malware over the Internet and should condition employees to always carefully check the domain to make sure it is the legitimate vendor's website. Rather than develop a security awareness training program from scratch, businesses should consider using a vendor that can provide a comprehensive training platform that is constantly updated with new training content covering new attack methods and scams. A security

awareness training program should run continuously, to build awareness, teach security best practices, and ensure that employees are constantly reminded of the importance of security.

In addition to training, technical measures should be implemented. A web filter should be used to prevent access to known malicious web pages and block downloads of executable files from the Internet, with policies implemented that require any software to be provided through or by the IT team. TitanHQ can help to improve your defenses against malware with a suite of cybersecurity solutions, including the SafeTitan security awareness training and phishing simulation platform, the WebTitan web filter to prevent access to malicious websites, SpamTitan email security with sandboxing to block malicious emails, and PhishTitan to improve phishing detection and mediation for businesses that use Microsoft 365.

For more information about these and other cybersecurity solutions from TitanHQ, give the sales team a call. All TitanHQ SaaS solutions are available on a free trial to allow you to test them in your own environment before making a purchase decision, with customer support provided throughout the trial.

Devastating Healthcare Cyberattack Started with a Malicious File Download from the Internet

by G Hunt | June 19, 2024 | Internet Security

Ascension, one of the largest private healthcare systems in the United States, fell victim to a ransomware attack on May 8, 2024, that forced systems offline, including patients' medical records which were not fully restored for a month. The attack caused massive disruption, and without access to electronic health records, staff were forced to record patient information manually.

Patient care was seriously affected, with delays in diagnosis and treatment, and the lack of access to medical records resulted in medical errors. Without technology to perform routine safety checks, patient safety was put at risk. The investigation into the attack is still ongoing, but evidence has already been found that files containing sensitive data were stolen in the attack. The scale of the data breach has yet to be determined but for a healthcare system as large as Ascension, the breach could be considerable.

The ransomware attack occurred as a result of a simple error by a single employee, who was tricked into downloading a malicious file from the internet. That file provided the attackers with a foothold in the network, from where they were able to launch a devastating ransomware attack. Ascension said it has no reason to believe that the file download was a malicious act and is satisfied that it was an honest mistake by the employee. Sadly, it is the type of mistake that frequently results in ransomware attacks and costly data breaches.

Ascension has not disclosed how the file was downloaded, whether it was from general web browsing, malvertising that directed the employee to a malicious website, or if they clicked a link in a phishing email. Regardless of how the employee arrived at the malicious site, the attack could have been prevented with the right technology in place. It is possible to protect against all of the above-mentioned methods of malware delivery with a web filter. WebTitan from TitanHQ is a DNS-based web filter for businesses to prevent employees from visiting websites hosting malware and to block the web-based component of phishing attacks.

WebTitan is fed threat intelligence to provide real-time protection against malicious websites. As soon as a malicious website is detected, it is added to the database and all WebTitan users are prevented from visiting that URL. WebTitan categorizes and blocks around 60,000 malware and spyware domains each day and if an attempt is made to visit one of those URLs, whether it is via a link in an email, malvertising, or general web browsing, the attempt is blocked and the user is directed to a locally hosted block page.

WebTitan is updated constantly with vast click stream traffic from actively visited URLs from 500 million end users, and the data is used to categorize websites. WebTitan users can then place restrictions on 53 categories of websites that employees can visit on their work devices, eliminating risks from common sources of malware such as torrent and file-sharing sites for which there is no business reason for access. Further, as an additional protection against malware, WebTitan can be configured to block downloads of certain file types from the internet, such as executable files that are commonly used to deliver malware. For the majority of employees, there is rarely a business need to download executable files.

Malware is commonly delivered via email, either via attachments containing malicious scripts and macros or via embedded hyperlinks. It is important to have an advanced email security solution in place to block this method of malware delivery. SpamTitan is a cloud-based anti-spam service that protects against known malware using twin antivirus engines that scan attachments for the signatures of malware. To protect against novel malware threats, SpamTitan incorporates a Bitdefender-powered email sandbox, where suspicious messages are sent for deep inspection. An email sandbox is key to blocking malware threats and essential due to the volume of novel malware variants now being distributed.

While technological solutions are essential, it is also important to provide security awareness training to the workforce to improve awareness of cyber threats and teach security best practices. This is another area where TitanHQ can help. SafeTitan is a comprehensive security awareness training platform and phishing simulator that is proven to reduce susceptibility to phishing attacks that helps businesses develop a human firewall and combat the many threats that target employees.

For more information on improving your defenses against malware and phishing threats, give the TitanHQ team a call. All TitanHQ cybersecurity solutions are also available on a free trial to allow you to put them to the test before making a purchase decision.

Torrent Sites Used to Deliver Dangerous Malware Packaged with Pirated Software

by G Hunt | May 31, 2024 | Internet Security

Downloading unofficial and pirated software from the Internet carries a significant risk of malware infections. Malware is often packaged with the installers or with the cracks/key generators that provide the serial keys or codes to activate the software.

Cybercriminals use a variety of methods for driving traffic to their malicious websites, including malicious Google Ads, adverts on other third-party ad networks, SEO poising to get their malicious sites appearing high in the search engine listings, and via torrent and warez sites. A warning has recently been issued about the latter by AhnLab Security Intelligence Center (ASEC).

The campaign identified by the researchers distributes Microsoft Office, Microsoft Windows, and the Hangul Word Processor. The pirated software is available through torrent sites and includes a professional-looking installer. The installer for Microsoft Office allows users to select the Office products they want to install in either the 32-bit or 64-bit version and select the language.

If the installer is run, the user will get the software they are looking for; however, in the background, a malware cocktail will be installed. The threat actor behind this campaign is distributing several different malware payloads, including coinminers, remote access trojans (RATs), downloaders, and anti-AV malware.

When the installer is run, an obfuscated .NET downloader is executed which connects to the attacker's Telegram/Mastadon channels and obtains a Google Drive or GitHub URL from where Base64 encrypted strings are obtained. Those strings are decrypted on the device and are PowerShell commands. Task Scheduler is used to execute the PowerShell commands, which install the malware. The scheduled tasks also allow the threat actor to consistently install other malware variants on the infected device.

By using Task Scheduler, the threat actor can reinstall malware if it is detected and removed, and since an updater is installed, the PowerShell commands can change. Even if the initial URLs are blocked, others will be added to ensure malware can still be delivered.

Initially, the threat actor was installing the updater together with either the Orcus RAT or the XMRig cryptocurrency miner. Orcus RAT provides the threat actor with remote control of an infected device, and has keylogging capabilities, can take screenshots, access the webcam, and exfiltrate data. XMRig is configured to only run when it is unlikely to be detected and will quit when system resource usage is high.

In the latest campaign, the threat actor also installs 3Proxy, which allows abuse of the infected device as a proxy, PureCrypter for downloading and executing additional malware payloads, and AntiAV malware, which disables antivirus and other security software by modifying the configuration files.

While this campaign appears to be targeting users in South Korea, it clearly shows the risks of downloading pirated software. Due to the inclusion of the updater and the installation of PureCrypter, remediation is difficult. Further, new malware variants are being distributed every week to evade detection.

Employees often download software to make it easier for them to do their jobs, and Torrent sites are a common source of unauthorized software. Businesses should therefore implement policies that prohibit employees from downloading software that has not been authorized by the IT department and should also implement controls to prevent Torrent and other software distribution sites from being accessed.

With TitanHQ's WebTitan DNS filter, blocking access to malicious and risky websites could not be simpler. Simply install the cloud-based web filter and configure the solution by using the checkboxes in the user interface to block access to these categories of websites. WebTitan is constantly updated with the latest threat intelligence to block access to known malicious websites, and it is also possible to block downloads of executable files from the Internet.

For more information on improving Internet security with a DNS-based web filter, give the TitanHQ team a call. WebTitan, like all other TitanHQ products, is available on a free trial, with product support provided to ensure you get the most out of the solution during the trial.

Discord Phishing Risk Increases with 50,000+ Malicious Links Detected in 6 Months

by G Hunt | May 30, 2024 | Phishing & Email Spam, Security Awareness

Phishing tactics are constantly changing and while email is still one of the most common ways of getting malicious content in front of end users, other forms of phishing are growing. Smishing (SMS phishing) has increased considerably in recent years, and vishing (voice phishing) is also common, especially for IT support scams.

Another method of malware delivery that has seen an enormous increase recently is the use of instant messaging and VoIP social platform Discord. Discord is a platform that has long been popular with gamers, due to being able to create a server with voice and text for no extra cost, both of which are necessary for teamspeak in gaming. While gamers still account for a majority of users, usage for non-gaming purposes is growing.

The platform is also proving popular with cybercriminals who are using it for phishing campaigns and malware distribution. According to Bitdefender, the antivirus company whose technology powers the SpamTitan email sandboxing feature, more than 50,000 malicious links have been detected on Discord in the past 6 months. Around a year ago, a campaign was detected that used Discord to send links to a malicious site resulting in the delivery of PureCrypter malware – a fully featured malware loader that is used for distributing information stealers and remote access trojans.

Discord responded to the misuse of the platform and implemented changes such as adding a 24-hour expiry for links to internally hosted files, which made it harder for malicious actors to use the platform for hosting malware. While this move has hampered cybercriminals, the platform is still being used for malware distribution. One of the latest malicious Discord campaigns is concerned with obtaining credentials and financial information rather than distributing malware.

The campaign involves sending links that offer users a free Discord Nitro subscription. Discord Nitro provides users with perks that are locked for other users, such as being able to use custom emojis anywhere, set custom video backgrounds, HD video streaming, bigger file uploads, and more. Discord Nitro costs $9.99 a month, so a free account is attractive.

If the user clicks the link in the message, they are directed to a fake Discord website where they are tricked into disclosing credentials and financial information. Other Discord Nitro lures have also been detected along the same theme, offering advice on how to qualify for a free Discord Nitro subscription by linking to other accounts such as Steam. According to Bitdefender, 28% of detected malicious uses are spam threats, 27% are untrusted, around 20% are phishing attempts and a similar percentage involve malware distribution.

Any platform that allows direct communication with users can be used for phishing and other malicious purposes. Security awareness training should cover all of these attack vectors and should get the message across to end users that they always need to be on their guard whether they are on email, SMS, instant messaging services, or the phone. By running training courses continuously throughout the year, businesses can develop a security culture by training their employees to be constantly on the lookout for phishing and malware threats and developing the skills that allow them to identify threats.

Developing, automating, and updating training courses to include information on the latest threats, tactics techniques, and procedures used by threat actors is easy with the SafeTitan security awareness training platform. SafeTitan makes training fun and engaging for end users and the platform has been shown to reduce susceptibility to phishing and malware threats by up to 80%.

If you are not currently running a comprehensive security awareness training program for your workforce or if you are looking to improve your training. Give the TitanHQ team a call and ask about SafeTitan. SafeTitan is one product in a suite of cloud-based security solutions for businesses and managed service providers, which includes an enterprise spam filter, a malicious file sandbox for email, a DNS-based web filter, email encryption, email archiving, and phishing protection for M365.

How to Protect Against Advanced Email and SMS Phishing Threats

by G Hunt | May 27, 2024 | Phishing & Email Spam, Security Awareness, Spam Advice

Email phishing is the most common form of phishing, with email providing threat actors with an easy way of getting their malicious messages in front of employees. Phishing emails typically include a URL along with a pressing reason for clicking the link. The URLs are often masked to make them appear legitimate, either with a button or link text relevant to the lure in the message. Email attachments are often added to emails that contain malicious scripts for downloading a variety of malicious payloads, or links to websites where malware is hosted.

While there are many email security solutions available to businesses, many lack the sophistication to block advanced phishing threats as they rely on threat intelligence, antivirus software, and reputation checks. While these are important and effective at blocking the bulk of phishing and malspam emails, they are not effective at blocking zero-day attacks, business email compromise, and advanced phishing threats.

More advanced features include email sandboxing for detecting and quarantining zero-day malware threats and malicious scripts, greylisting for increasing the spam catch rate, and AI and machine learning capabilities that can assess messages and identify threats based on how they differ from the messages that are typically received by the business. SpamTitan, a cloud-based anti-spam service from TitanHQ, has these features and more. Independent tests have shown that the solution blocks more than 99.99% of spam emails, 99.95% of malware, and more than 99.91% of phishing emails. SpamTitan can be provided as a hosted email filter or as a gateway spam filter for installation on-premises on existing hardware, serving as a virtual anti-spam appliance.

Microsoft 365 users often complain about the phishing catch rate of the protections provided by Microsoft, which are EOP only for most licenses and EOP and Defender for the most expensive licenses. While these protections are effective at blocking spam and known malware, they fall short of what is required for blocking advanced threats. To improve Microsoft 365 security and block the threats that Microsoft misses, TitanHQ has developed PhishTitan. PhishTitan augments Microsoft 365 defenses and is the easiest way of improving the Office 365 spam filter. These advanced defenses are now vital due to the increase in attacks. The Anti-Phishing Working Group (APWG) has reported that more phishing attacks were conducted in 2023 than ever before.

Massive Increase in Text Message Phishing Scams

Blocking email phishing attempts is straightforward with advanced email security solutions, which make it much harder for phishers to get their messages in front of employees. One of the ways that threat actors have adapted is by switching to SMS phishing attacks, which no email security solution can block. APWG has reported a major increase in SMS-based phishing attempts.

A recent study attempted to determine the extent to which SMS phishing is being used. Researchers used SMS gateways – websites that allow users to obtain disposable phone numbers – to obtain a large number of phone numbers for the study. They then waited to see how long it took for SMS phishing messages to be received. The study involved 2,011 phone numbers and over 396 days the researchers received an astonishing 67,991 SMS phishing messages, which averages almost 34 per number. The researchers analyzed the messages and identified 35,128 unique campaigns that they associated with 600 phishing operations. Several of the threat actors had even set up URL shortening services on their own domains to hide the destination URLs. With these shortening services, the only way to tell that the domain is malicious is to click the link.

Blocking SMS phishing threats is difficult for businesses and the primary defense is security awareness training. SMS phishing should be included in security awareness training to make employees aware of the threat, as it is highly likely that they will encounter many SMS phishing threats. The SafeTitan security awareness platform makes creating training courses simple and the platform includes training content on all types of threats, including SMS, voice, and email phishing. With SafeTitan it is easy to create and automate campaigns, as well as deliver training in real-time in response to employee errors to ensure training is provided when it is likely to have the greatest impact – immediately after a mistake is made.

Sophisticated Phishing Campaign Abuses Cloudflare Workers

by G Hunt | May 26, 2024 | Phishing & Email Spam, Security Awareness

Cloudflare Workers is being abused in phishing campaigns to obtain credentials for Microsoft, Gmail, Yahoo!, and cPanel Webmail. The campaigns identified in the past month have mostly targeted individuals in Asia, North America, and Southern Europe, with the majority of attacks conducted on organizations in the technology, finance, and banking sectors.

Cloudflare Workers is part of the Cloudflare Developer Platform and allows code to be deployed and run from Cloudflare's global network. It is used to build web functions and applications without having to maintain infrastructure. The campaigns were identified by researchers at Netskope Threat Labs. One campaign uses a technique called HTML smuggling, which involves abusing HTML5 and JavaScript features to inject and extract data across network boundaries. This is a client-side attack where the malicious activities occur within the user's browser. HTML smuggling is most commonly associated with malware and is used to bypass network controls by assembling malicious payloads on the client side. In this case, the malicious payload is a phishing page.

The phishing page is reconstructed in the user's browser, and they are prompted to log in to the account for which the attacker seeks credentials, such as their Microsoft account. When the victim enters their credentials, they will be logged in to the legitimate website and the attacker will then collect the tokens and session cookies.

Another campaign uses adversary-in-the-middle (AitM) tactics to capture login credentials, cookies, and tokens, and allow the attackers to compromise accounts that are protected with multi-factor authentication. Cloudflare

Workers is used as a reverse proxy server for the legitimate login page for the credentials being targeted. Traffic between the victim and the login page is intercepted to capture credentials as well as MFA codes and session cookies. The advantage of this type of attack is the user is shown the exact login page for the credentials being targeted. That means that the attacker does not need to create and maintain a copy of the login page.

When the user enters their credentials, they are sent to the legitimate login page by the attacker, and the response from the login page is relayed to the victim. The threat actor's application captures the credentials and the tokens and cookies in the response. In these CloudFlare Workers phishing campaigns, users can identify the scam by looking for the *.workers.dev domain and should be trained to always access login pages by typing the URL directly into the web browser.

Defending against sophisticated phishing attacks requires a combination of security measures including an email security solution with AI/machine learning capabilities and email sandboxing, regular security awareness training, and web filtering to block the malicious websites and inspecting HTTP and HTTPS traffic. For more information on improving your defenses, give the TitanHQ team a call.

Two Dozen Healthcare Email Accounts Compromised in Targeted Phishing Campaign

by G Hunt | April 25, 2024 | Email Scams, Phishing & Email Spam

Many phishing campaigns involve indiscriminate emails that are sent in high volume in the hope that some recipients will respond. These campaigns tend to involve lures that are likely to be opened by as many users as possible such as missed deliveries, security warnings about unauthorized account access, and payments that will soon be applied to accounts. This spray-and-pray tactic is not nearly as effective as more tailored campaigns targeting specific types of users, and to make up for this, the campaigns involve huge volumes of messages. These campaigns are relatively easy for email security solutions to detect.

Phishing campaigns that target employees in a single organization can be much harder to identify. The threat actor tailors the message to the organization being targeted, and even to specific employees in the organization. These campaigns often use compromised vendor email accounts, with the emails being sent from trusted domains. There is a much greater chance of these emails landing in inboxes and the emails being opened by employees. Campaigns such as this can be highly effective and often result in many email accounts in the organization being compromised.

A recent example of this type of attack and the impact it can have comes from California. The Los Angeles County Department of Health Services, an integrated health system that operates public hospitals and clinics in L.A. County, was targeted in a phishing campaign between February 19, 2024, and February 20, 2024. The emails appeared to have been sent by a trusted sender, landed in inboxes, and were opened by many employees. The emails contained a hyperlink that directed users to a website where they were told they needed to enter their login credentials. 23 employees fell for the scam and entered their credentials.

The credentials were captured, and the threat actor was able to access the employees' email accounts, which contained sensitive patient data such as names, dates of birth, contact information, medical record numbers, dates of service, medical information, and health plan information. While the information exposed in the attack could

not be used for identity theft – Social Security numbers were not compromised – the attacker gained access to information that could be used for medical identity theft. The patients affected could also be targeted in very convincing phishing campaigns to obtain further information such as Social Security numbers. Similar attacks have been reported by other healthcare organizations where the email accounts contained vast amounts of data, including tens of thousands of Social Security numbers and sensitive financial information.

After attacks such as this, additional security awareness training is provided to the workforce to raise awareness of the threat from phishing; however, the provision of comprehensive training regularly throughout the year will go a long way toward ensuring that attacks such as this do not succeed and that if they do, the resultant data breach is far less severe.

TitanHQ's SafeTitan security awareness training platform allows organizations to conduct comprehensive training continuously, and since each training module is a maximum of 10 minutes, it is easy to fit the training into busy workflows. The training platform has a huge range of content, covering a broad range of threats, and when programs are run continuously and employees complete a few training modules a month, susceptibility to phishing drops considerably, especially when the SafeTitan phishing simulator is also used. The simulator includes templates taken from recent real-world phishing campaigns. If a user responds to one of these simulations, they are immediately told where they went wrong and are required to complete a training module relevant to that threat.

End-user security awareness training is an important part of your cybersecurity arsenal, but it is also vital to block as many phishing emails as possible. TitanHQ's SpamTitan email security is an advanced, AI and machine learning-driven anti-spam solution that blocks more than 99.9% of spam email and phishing threats. The solution includes twin antivirus engines for blocking known malware, and sandboxing for blocking zero-day threats, and is a highly effective spam filter for Office 365. With SafeTitan security awareness training and an advanced Microsoft 365 spam filter from TitanHQ, businesses will be well protected from phishing threats.

All TitanHQ solutions are intuitive, easy to use, and can be set up in just a few minutes and are available on a free trial to allow you to test them out for yourself before making a purchase decision. Independent reviews from genuine users of TitanHQ solutions show SpamTitan is much loved by users. On G2 reviews, SpamTitan is consistently given 5-star reviews by end users, who rate it the best spam filter for Outlook due to its effectiveness, low cost, ease of use, and the excellent customer service from the TitanHQ team.

SafeTitan and SpamTitan are available on a free trial to allow you to test them out for yourself before making a purchase decision. Give the TitanHQ team a call today to take the first step toward improving your phishing defenses.

Remcos RAT Now Distributed in Spam Email Using VHD Attachments

by G Hunt | April 24, 2024 | Phishing & Email Spam

Cybercriminals are constantly evolving their tactics for delivering malware and one of the most recent changes concerns the Remcos RAT. Remcos was developed by Breaking Security as a legitimate remote administration tool that can be used for network maintenance, system monitoring, surveillance, and penetration testing; however, the tool has been weaponized to create the Remcos Remote Access Trojan (RAT).

The Remocos RAT has extensive capabilities and has been used by cybercriminals since 2016. The malware allows threat actors to take control of systems and maintain persistent, highly privileged remote access. The malware can be used for a range of purposes, with threat actors commonly using it for credential theft, man-in-the-middle internet connections, and to create botnets of infected devices that can be used for distributed denial of service attacks (DDoS).

The Remcos RAT is distributed in spam email campaigns. Since 2016, the most common method for distributing the malware used spam emails with malicious Office attachments. Social engineering techniques were used to trick users into opening the files and enabling macros; however, campaigns have recently been detected that deliver the malware via weaponized virtual hard disk (VHD) files.

Security awareness training often focuses on teaching users to be careful when opening Office files and other file types commonly associated with malware distribution. The change to a more unusual file type could result in the file being opened, and VHD files are less likely to be identified as malicious by email security solutions.

An analysis of the extracted VHD files revealed a shortcut file that contained a PowerShell command line that executed a malicious script that ultimately delivered the Remcos RAT via a sophisticated multi-stage delivery method designed to evade security solutions. Once installed, the malware can log keystrokes, take screenshots, and exfiltrate data to its command-and-control server. The malware also has mass-mailer capabilities and can send copies of itself via email from an infected device. According to Check Point, the Remcos RAT rose to the 4th most prevalent malware threat in March 2024.

The constantly changing tactics for distributing malware mean network defenders need cybersecurity solutions that can adapt and detect zero-day threats. SpamTitan is an advanced email filtering service with AI and machine learning-driven threat detection which is capable of identifying and blocking novel phishing and malware distribution methods. The machine learning algorithm uses predictive technology to identify previously unseen attacks, emails are scanned using twin antivirus engines, and suspicious file types are sent to a next-generation sandbox for behavioral analysis, ensuring even previously unseen malware variants can be identified and blocked.

SpamTitan scans all inbound emails and also includes an outbound email filter to identify malicious emails that are sent from compromised email accounts and by malicious insiders. SpamTitan also has data loss protection capabilities, allowing IT teams to detect and block internal data loss. If your corporate email filter does not include advanced threat protection including AI-driven detection and sandboxing, or if you rely on Microsoft’s anti-spam and anti-phishing protection, sophisticated threats such as zero-day attacks are unlikely to be blocked and your business will be at risk.

Give the TitanHQ team a call today to find out more about SpamTitan. SpamTitan is delivered as a cloud-based anti-spam service that integrates seamlessly with Microsoft 365 to improve protection, or as a gateway solution for on-premises protection, which can be installed on existing hardware as a virtual anti-spam appliance.

Financial Institutions Targeted in Phishing Campaign That Delivers the JSOutProx RAT

by G Hunt | April 17, 2024 | Email Scams, Phishing & Email Spam

A phishing campaign has been running since late March that tricks people into installing a new version of the remote access trojan, JSOutProx. JSOutProx was first identified in 2019 and is a backdoor that utilizes JavaScript and .NET that allows users to run shell commands, execute files, take screenshots, control peripheral devices, and download additional malware payloads. The malware is known to be used by a threat actor tracked as Solar Spider, which mostly targets financial institutions in Central Europe, South Asia, Southeast Asia, and Africa, with the latest version of the malware also being used to target organizations in the Middle East.

The malware has mostly been used on banks and other financial institutions. If infected, the malware collects information about its environment and the attackers then download any of around 14 different plug-ins from either GitHub or GitLab, based on the information the malware collects about its operating environment. The malware can be used to control proxy settings, access Microsoft Outlook account details, capture clipboard content, and steal one-time passwords from Symantec VIP.

Like many other remote access trojans, JSOutProx is primarily delivered via phishing emails. A variety of lures have been used in the phishing emails but the latest campaign uses fake notifications about SWIFT payments in targeted attacks on financial institutions and MoneyGram payment notifications in attacks on individuals, which aim to trick the recipients into installing the malware.

The latest campaign uses JavaScript attachments that masquerade as PDF files of financial documents contained in .zip files. If the user attempts to open the fake PDF file, the JavaScript is executed deploying the malware payload. The main aim of the campaign is to steal user account credentials, gather sensitive financial documents, and obtain payment account data, which can either be used to make fraudulent transactions or be sold to other threat actors on the dark web. Email accounts are often compromised which can be leveraged in Business Email Compromise (BEC) attacks to steal funds from clients. According to VISA, “The JSOutProx malware poses a serious threat to financial institutions around the world, and especially those in the AP region as those entities have been more frequently targeted with this malware.”

Since phishing is the main method of malware delivery, the best defense against attacks is advanced anti-spam software and end-user security awareness training. JSOutProx malware is able to bypass many traditional anti-spam solutions and anti-virus software due to the high level of obfuscation. The best defense is an anti-spam solution with AI and machine learning capabilities that can identify the signs of malicious emails by analyzing message headers and message content to determine how they deviate from the emails typically received by the business and also search for the signs of phishing and malware delivery based on the latest threat intelligence.

To identify the malicious attachments, an anti-spam solution requires sandboxing. Any messages that pass standard antivirus checks are sent to the sandbox where behavior is analyzed to identify malicious actions, rather than relying on malware signatures for detection. SpamTitan can extract and analyze files in compressed archives such as .zip and .rar files and in recent independent tests, SpamTitan achieved a phishing catch rate of 99.914%, a malware catch rate of 99.511%, with a false positive rate of 0.00%. SpamTitan from TitanHQ is delivered as either a hosted anti-spam service or an anti-spam gateway that is installed on-premises on existing hardware. SpamTitan has been developed to be easy to implement and use and meet the needs of businesses of all sizes and managed service providers.

Phishing emails target employees so it is important to teach them how to identify phishing emails. Due to the fast-changing threat landscape, security awareness training should be provided continuously to the workforce, and phishing simulations should be conducted to give employees practice at identifying threats. SafeTitan from TitanHQ can be used to easily create effective training programs that run continuously throughout the year and keep employees up to date on the latest threats and tactics, techniques, and procedures used by malicious actors. SafeTitan also delivers relevant training in real-time in response to security mistakes and phishing simulation failures. Check out these anti-spam tips for further information on improving your defenses against phishing and get in touch with TitanHQ for more information on SpamTitan email security and the SafeTitan security awareness training platform.

Sophisticated Phishing Campaign Delivers Rats via SVG File Attachments

by G Hunt | April 15, 2024 | Email Scams, Phishing & Email Spam

A sophisticated phishing campaign has been detected that is being used to deliver a variety of Remote Access Trojan (RAT) malware, including Venom RAT, Remcos RAT, and NanoCore RAT, as well as a stealer that targets cryptocurrency wallets. The campaign uses email as the initial access vector with the messages purporting to be an invoice for a shipment that has recently been delivered. The emails include a Scalable Vector Graphics (SVG) file attachment – an increasingly common XML-based vector image format.

If the file is executed, it will drop a compressed (zip) file on the user's device. The zip file contains a batch file that has been created with an obfuscation tool (most likely BatCloak) to allow it to evade anti-virus software. If not detected as malicious, a ScrubCrypt batch file is unpacked – another tool used to bypass antivirus protections – which delivers two executable files that are used to deliver and execute the RAT and establish persistence. This method of delivery allows the malware to evade AMSI (Antimalware Scan Interface) and ETW (Event Tracing for Windows) antivirus protections.

One of the primary payloads is Venom RAT, which establishes a connection with its command and control (C2) server, transmits sensitive information gathered from the compromised device and runs commands from its C2 server. Venon RAT can download additional modules and malware payloads, including a stealer malware that targets folders associated with cryptocurrency wallets and applications including Atomic Wallet, Electrum, Exodus, Foxmail, and Telegram.

The sophisticated nature of this campaign and the obfuscation used to hide the malicious payloads from traditional antivirus software demonstrates the need for advanced email defenses and end-user training. Email security solutions that rely on malware signatures are easily bypassed, which is why it is important to use an anti-spam solution that incorporates sandboxing for blocking malware and AI and machine learning capabilities to identify malicious emails.

SpamTitan uses AI and machine learning algorithms to detect phishing emails that other solutions miss – including Microsoft's basic and advanced anti-phishing mechanisms for Microsoft 365. SpamTitan includes Sender Policy Framework (SPF), SURBL's, RBL's, Bayesian analysis, and more, and the machine learning algorithms can detect email messages that deviate from the typical messages received by a business and can identify header anomalies, address spoofing, and suspect email body content. All inbound messages are subjected

to standard and advanced malware checks, including scans using twin anti-virus engines and email sandboxing. If all anti-malware checks are passed, including unpacking and analyzing compressed files, messages are sent to the sandbox for behavioral analysis.

In the cloud-based sandbox, malicious actions are identified such as attempts to deliver additional files as is commonly seen in multi-stage attacks and C2 calls. In recent independent tests (Virus Bulletin), SpamTitan achieved a phishing catch rate of 99.914%, a malware catch rate of 99.511%, and a false positive rate of 0.00%. With phishing attacks becoming more sophisticated you need to have sophisticated defenses. With email security protection provided by SpamTitan and security awareness training delivered using TitanHQ's award-winning SafeTitan security awareness training and phishing simulation platform you will be well protected from email-based attacks.

Give the TitanHQ team a call today to find out more about how you can improve your defenses against email-based attacks with sandboxing technology and how to add more layers to your defenses to block the full range of cyberattacks.

TitanHQ's Anti-Phishing Solution Now Has Auto-Remediation Feature

by G Hunt | March 31, 2024 | Industry News, Network Security

TitanHQ has added a new auto-remediation feature to its Microsoft 365 anti-phishing solution, PhishTitan, to better meet the needs of managed service providers (MSP) and M365 administrators.

According to Statista, more than two million companies worldwide use Microsoft 365, including more than 1.3 million in the United States. Given the number of companies that use Microsoft 365, it is naturally a big target for cybercriminals and nation-state actors. If threat actors can steal M365 credentials, they can access a treasure trove of valuable business data and gain a foothold for more extensive and damaging attacks. Microsoft offers protection against spam, phishing, malware, and business email compromise attacks, but the best level of protection is only available with its costly E5 premium license, which is prohibitively expensive for many small businesses. Even companies that can afford this costly license do not get cutting-edge protection against phishing and BEC attacks.

To consistently block sophisticated phishing attempts, BEC attacks, and zero-day threats, businesses need more advanced protection than Microsoft can offer, and many turn to PhishTitan from TitanHQ – an integrated Cloud Email Security Solution (ICES) that provides cutting-edge protection against the most damaging, sophisticated phishing threats, BEC, account takeover, VIP impersonation, and zero-day attacks. In recent Virus Bulletin Tests, the engine that powers PhishTitan achieved an exceptional spam catch rate of 99.983%, a malware catch rate of 99.511%, and a phishing catch rate of 99.914%, with zero false positives. PhishTitan was shown to outperform Microsoft's highest level of protection. For every 80,000 emails received, PhishTitan blocks 20 more unique and sophisticated attacks than Microsoft's E5 filtering option.

The latest update to PhishTitan adds a new auto-remediation feature, which allows administrators to tailor the management of malicious emails based on the severity level. When a threat is detected, a banner is added to the email that warns the user about the threat; however, auto-remediation allows administrators to apply rules to deal with these messages according to the threat level, such as automatically diverting the emails to the junk folder.

This feature acts like a virtual SOC and minimizes the risk to end users, especially individuals who tend to ignore email banners.

Auto-remediation is just one of the new features PhishTitan has gained since its launch. PhishTitan has also received an update to protect users from the growing threat of QR code phishing attacks (QRishing). QR codes are problematic for many anti-spam and anti-phishing solutions, as they cannot decipher the URLs in QR codes and check the destination URL, which is why cybercriminals are increasingly using QR codes in their phishing emails. PhishTitan can analyze the URLs encoded in QR codes, assess the risk, and notify end users.

PhishTitan also supports allow-listing, which administrators can use to automatically white-list trusted senders to make sure that their emails are always delivered, and notifications can also be fed into Microsoft Teams. Since administrators can spend a considerable amount of time in the application, a dark mode has been added to improve the user experience, and many more updates are planned and will be rolled out soon.

“We are excited to introduce Auto Remediation, QR code protection, and many additional powerful new features to our valued customers. At TitanHQ, we collaborate closely with partners to develop tailored solutions addressing critical customer IT security challenges,” said TitanHQ CEO, Ronan Kavanagh. “PhishTitan provides MSPs with an unmatched value proposition, featuring effortless deployment and lucrative recurring revenue streams, ultimately delivering a positive return on investment.”

If you want to improve protection against email threats or have any questions about PhishTitan, give the TitanHQ team a call. TitanHQ also offers award-winning DNS filtering, spam filtering, email encryption, email archiving, security awareness training, and phishing simulation solutions, all of which are available on a free trial.

TitanHQ Achieves Virus Bulletin VBSpam+ Certification with 99.91% Phishing Catch Rate in Latest Tests

by G Hunt | March 29, 2024 | Phishing & Email Spam, Spam Software

TitanHQ has claimed a Top 3 position in a recent Virus Bulletin email security test, achieving an exceptional 99.98% spam catch rate and 99.91% phishing catch rate for the cutting-edge filtering engine that powers the SpamTitan (email security) and PhishTitan (phishing protection) solutions, earning TitanHQ the prestigious VBSpam+ certification for the products.

Virus Bulletin is a security information portal and independent testing and certification body that has earned a formidable reputation within the cybersecurity community for providing security professionals with intelligence about the latest developments in the global threat landscape. Virus Bulletin conducts regular tests of security solutions to determine how well they perform at detecting and blocking threats, and for more than 20 years has been benchmarking cybersecurity solutions. Virus Bulletin’s public certifications cover all types of security threat protection, including anti-spam and anti-phishing solutions for enterprises.

In the Q1, 2024 tests, Virus Bulletin assessed nine comprehensive email security solutions, including TitanHQ’s email security suite which comprises SpamTitan and PhishTitan. The email security solutions were put to the test to assess how effective they are at blocking unsolicited and unwanted spam emails and malicious messages of all types. TitanHQ’s solutions achieved exceptional scores at blocking spam and phishing emails, with a spam catch

rate of 99.983%, a malware catch rate of 99.511%, and a phishing catch rate of 99.914% with zero false positives. The final score for the Q1, 2024 tests was 99.983, cementing TitanHQ's position as a leading provider of anti-phishing and anti-spam solutions for managed service providers and businesses.

"This test reaffirms TitanHQ's unrivaled prowess in spam and phishing protection—we stand as the first choice for combating phishing attempts and spam infiltrations," said Ronan Kavanagh, CEO at TitanHQ. "Our customers need not settle for anything less. With TitanHQ solutions, they receive unparalleled defense against phishing and spam and experience minimal false positives.

While there are many ways that cybercriminals and nation state actors breach company networks and gain access to sensitive data, phishing is the leading initial access vector. Despite phishing being such a prevalent threat, many businesses lack security solutions that can consistently identify and block these malicious messages, which results in costly compromises, data breaches, and devastating ransomware attacks. According to one study by researchers at CoreView on 1.6 million Microsoft 365 users, 90% lacked essential security protections that can combat threats such as phishing.

While Microsoft has security solutions that can block spam and phishing emails, they are unable to block advanced phishing threats. PhishTitan has been developed to work seamlessly with M365 and catch the phishing threats that M365 misses. Even Microsoft's most advanced anti-phishing protection, the costly E5 premium security offering, fails to block many advanced threats. Testing has shown that for every 80,000 emails received, PhishTitan identifies and blocks 20 unique, sophisticated phishing attempts that Microsoft's top solution misses, and many businesses cannot afford Microsoft's top level of protection and are reliant on its basic anti-spam and anti-phishing protection.

If you want to improve your defenses against phishing and malware and block more spam emails, give the TitanHQ team a call and ask about SpamTitan and PhishTitan. Both email filtering solutions are available on a free trial, so you can put them to the test and see for yourself the difference they make.

Tycoon 2FA Phishing Kit Targets M365 and Gmail Credentials and Bypasses MFA

by G Hunt | March 27, 2024 | Phishing & Email Spam

Phishing is one of the most common methods used to gain access to credentials; however, businesses are increasingly implementing multi-factor authentication (MFA) which adds an extra layer of protection and means stolen credentials cannot be used on their own to gain access to accounts. An additional authentication factor is required before access to the account is granted. While any form of MFA is better than none, MFA does not protect against all phishing attacks. There are several popular phishing-as-a-service (PhaaS) platforms that can steal credentials and bypass MFA including LabHost, Greatness, and Robin Banks. For a relatively small fee, any cybercriminal looking to compromise accounts can use the PhaaS platform and gain access to MFA-protected accounts.

A relatively new PhaaS platform has been growing in popularity since its discovery in October 2023 which has been causing concern in the cybersecurity community. Dubbed Tycoon 2FA, the PhaaS platform is being offered through private Telegram groups. Like many other PhaaS platforms, Tycoon 2FA uses adversary-in-the-middle

(AiTM) tactics to steal MFA tokens, allowing access to be gained to accounts. The phishing kit uses at least 1,100 domains and has been used in thousands of phishing attacks.

Like most phishing attacks, initial contact is made with end users via email. The messages include a malicious link or a QR code. QR codes are popular with phishers as they communicate a URL to the end user and are difficult for email security solutions to identify as malicious. To ensure that the malicious URLs are not detected by security solutions, after clicking the link or visiting the website via the QR code, the user must pass a security challenge (Cloudflare Turnstile). The web page to which the user is directed targets Microsoft 365 or Gmail credentials. The user's email address is captured and used to prefill the login page, and when the user enters their password it is captured and they are directed to a fake MFA page.

The phishing kit uses a reverse proxy server that relays the user's credentials to the legitimate service being targeted in real-time and similarly captures the session cookie when the MFA challenge is passed. The user is unlikely to recognize that their account has been compromised as they are redirected to a legitimate-looking page when the MFA mechanism is passed. According to the researchers, many different threat actors have been using the kit for their phishing campaigns, with the Tycoon 2FA operators having received almost $395,000 in payments to their Bitcoin wallet as of March 2024. The price of the phishing kit is $120 for 10 days of usage which shows how popular the platform is with cybercriminals.

PhaaS platforms allow cybercriminals to conduct sophisticated attacks and bypass MFA without having to invest time and money setting up their own infrastructure they significantly lower the entry barrier for conducting MFA-bypassing phishing attacks. An advanced spam filtering service such as SpamTitan Plus will help to prevent malicious emails from reaching inboxes, and is an ideal spam filter for MSPs looking to provide the best level of protection for their clients. The SpamTitan suite of email security solutions combines phishing, spam, and antivirus filtering and independent tests show a spam block rate of 99.983% and a malware block rate of 99.51%.

PhishTitan from TitanHQ greatly improves protection against more advanced phishing campaigns such as those that use QR codes. Employees should be provided with regular security awareness training to help them identify and avoid phishing messages, and businesses should consider using phishing-resistant MFA rather than more basic forms of 2-factor authentication that use SMS or one-time passwords, which phishing kits such as Tycoon 2FA can easily bypass.

TitanHQ Expands Global Footprint into Africa with Strategic Alliance with Equinox Technologies

by G Hunt | March 26, 2024 | Industry News

TitanHQ has announced it has signed a new partnership agreement with Equinox Technologies which will see TitanHQ's cybersecurity solutions offered throughout Africa. Equinox Technologies is a pan-African, tech-enabled, business service provider that provides a range of services to more than 40 countries in Africa from its operational hubs in Abuja, Nigeria; Cape Town, South Africa; Nairobi, Kenya; and Tunis, Tunisia. Equinox Technologies helps businesses of all sizes expand and invest seamlessly across international borders through the provision of business-critical administrative, security, and compliance support. The services provided include enterprise mobility management, software engineering, IT operations, digital services, and cybersecurity.

The strategic alliance with TitanHQ will see Equinox Technologies act as a value-added distributor, packaging TitanHQ solutions with other products and services to meet its clients' cybersecurity and compliance needs and better protect them from the rapidly evolving landscape of cyber threats. Under the new agreement, Equinox Technologies will become the exclusive distributor of TitanHQ solutions in Africa, further expanding TitanHQ's global footprint.

Equinox Technologies will help its clients improve email security by offering TitanHQ's cloud-based anti-spam service (SpamTitan), phishing protection solution (PhishTitan), and email encryption solution (EncryptTitan), protection from web-based threats through TitanHQ's DNS filtering solution (WebTitan), threats that target employees with TitanHQ's security awareness training and phishing simulation platform (SafeTitan); and help them meet their email retention and compliance obligations through TitanHQ's email archiving solution (ArcTitan).

"This collaboration signifies Equinox Technologies' commitment to fortifying its cybersecurity offerings," said TitanHQ CEO, Ronan Kavanagh. "Together, Equinox Technologies and TitanHQ will be able to shield African companies from the constantly evolving landscape of cyber threats through a comprehensive suite of security solutions."

Facebook Messages Used to Distribute Snake Infostealer Malware

by G Hunt | March 20, 2024 | Phishing & Email Spam

Malware is often distributed via email or websites linked in emails, and advanced email security solutions such as SpamTitan Plus can protect you by preventing the messages from reaching inboxes. SpamTitan Plus uses dual antivirus engines to detect known malware and sandboxing to identify and block zero-day malware threats. SpamTitan Plus also rewrites URLs, uses predictive analysis to identify suspicious URLs, and blocks those URLs to prevent users from reaching the websites where malware is hosted. To get around email security solutions, cybercriminals use other methods for making initial contact with end users, and instant messaging services are a popular alternative.

Researchers at Cybereason recently identified a malware distribution campaign that distributes a Python-based information stealer via Facebook messages. The infostealer has been dubbed Snake and has been developed to steal credentials and other sensitive information. The campaign was first detected in the summer of 2023 and targets businesses. The messages use lures such as complaints and offers of products from suppliers to trick users into visiting a link and downloading a file. As is common with malware distribution campaigns, the threat actor uses legitimate public repositories for hosting the malicious file, such as GitHub and GitLab. The file to which the user is directed is a compressed file and, if extracted, will lead to the execution of a first-stage downloader. The first-stage downloader fetches a second compressed file, extracts the contents, and executes a second downloader, which delivers the Python infostealer.

Three different variants of the infostealer have been identified, all of which gain persistence via the StartUp folder. Each variant targets web browsers, including Brave, Chromium, Chrome, Edge, Firefox, Opera, and the Vietnamese CoC CoC browser, with the latter and other evidence suggesting that the campaign is being conducted

by a Vietnamese threat actor. All three variants also target Facebook cookies. The gathered data and cookies are exfiltrated in a .zip file via the Telegram Bot API or Discord.

One way of blocking these attacks is to use a web filter to block access to instant messaging services that are not required for business purposes, including Facebook Messenger. With WebTitan it is possible to block Messenger without blocking the Facebook site, and controls can be implemented for different users to allow users with responsibility for updating the organization's social media sites to access the platforms while preventing access for other users. It is also a good practice to use WebTitan to block downloads of executable files from the Internet to prevent malware delivery and stop employees from downloading and installing unauthorized software.

Dropbox Abused in Novel Phishing Attack to Obtain M365 Credentials

by G Hunt | March 14, 2024 | Phishing & Email Spam

The file hosting service Dropbox is being abused in a novel phishing campaign that exploits trust in the platform to harvest Microsoft 365 credentials. The campaign targeted 16 employees of an organization who received an email from the no-reply[@]dropbox.com account, a legitimate email account that is used by Dropbox. The emails included a link that directed the recipients to a Dropbox-hosted PDF file, which was named to appear as if it had been created by one of the organization's partners. If the PDF file was opened, the user would see a link that directs them to an unrelated domain – mmv-security[.]top. One of the employees was then sent a follow-up email reminding them to open the PDF file that was sent in the first email. They did, and they were directed to a phishing page that spoofed the Microsoft 365 login page. A couple of days later, suspicious logins were detected in the user's Microsoft 365 account from unknown IP addresses, which were investigated and found to be associated with ExpressVPN, indicating the attacker was using the VPN to access the account and mask their IP address.

Multifactor authentication was correctly configured on the account but this appears to have been bypassed, with the logins appearing to use a valid MFA token. After capturing credentials, the employee is thought to have unknowingly approved the MFA authentication request which allowed the account to be compromised. The attacker gained access to the user's email account and set up a new rule that moved emails from the organization's accounts team to the Conversation History folder to hide the malicious use of the mailbox. Emails were also sent from the account to the accounts team in an apparent attempt to compromise their accounts.

Phishing attacks are becoming increasingly sophisticated and much more difficult for end users to identify. Security awareness training programs often teach users about the red flags in emails they should look out for, such as unsolicited emails from unknown senders, links to unusual domains, and to be wary of any requests that have urgency and carry a threat should no action be taken. Impersonation is common in phishing attacks, but in this case, the impersonation went further with the emails sent from a valid and trusted account. That means that the email is more likely to be trusted and unlikely to be blocked by email security solutions, especially as the emails include a link to a file hosted on a trusted platform. This was also a staged attack, with follow-up emails sent, which in this case proved effective even though the second email was delivered to the junk email folder. The login page to which the user was directed looked exactly the same as the genuine login prompt for Microsoft 365, aside from the domain on which it was hosted.

Many businesses have configured multifactor authentication on their Microsoft 365 accounts, but as this attack demonstrates, MFA can be bypassed. The sophisticated nature of phishing attacks such as this demonstrates how important it is for businesses to have advanced defenses against phishing. TitanHQ's anti-phishing solutions use AI and a large language model (LLM) with proprietary threat intelligence currently not found in any other anti-phishing and anti-spam software solutions on the market. All emails are scanned – internal and external – for phrases and keywords that are unusual and could indicate malicious intent. All URLs are checked against various threat intelligence feeds to identify malicious URLs, and URLs are rewritten to show their true destination. The solution also learns from feedback provided by users and detection improves further over time. The curated and unique email threat intelligence data is unmatched in visibility, coverage, and accuracy, and TitanHQ's anti-spam and email security solutions feature sandboxing, where attachments are subjected to deep analysis in addition to signature-based anti-virus scanning. When a malicious email is detected, all other instances are removed from the entire M365 tenant.

If you want to improve your defenses against sophisticated phishing attacks give the TitanHQ team a call. If you are a Managed Service Provider looking for an easy-to-use solution to protect your clients from phishing and malware, look no further than TitanHQ. All solutions have been developed from the ground up to meet the needs of MSPs to better protect their customers from spam, phishing, malware, and BEC attacks.

CryptoChameleon Phishing Kit Targets FCC Employees and Cryptocurrency Platform Users

by G Hunt | March 5, 2024 | Phishing & Email Spam

A new phishing kit has been identified that is being used to target employees of the U.S. Federal Communications Commission (FCC) and the cryptocurrency platforms Binance and Coinbase, as well as users of cryptocurrency platforms such as Binance, Coinbase, Caleb & Brown, Gemini, Kraken, ShakePay, and Trezor.

A phishing kit is a set of tools and templates that allows threat actors to conduct effective phishing campaigns. These kits are marketed on the dark web to hackers and allow them to conduct phishing campaigns without having to invest time and money into setting up their own infrastructure. Phishing kits range from simple kits that provide phishing templates and cloned login pages, to more advanced kits that are capable of adversary-in-the-middle attacks that can defeat multifactor authentication. These kits significantly lower the entry barrier for conducting phishing campaigns as they require little technical expertise. Pay a relatively small fee and sophisticated phishing campaigns can be conducted in a matter of minutes.

The new phishing kit is called CryptoChameleon and allows users to create carbon copies of the single sign-on (SSO) pages that are used by the targeted businesses. Employees are used to authenticating through a single solution, through which they authenticate with many business applications. The kit also includes templates for phishing pages to harvest the credentials of cryptocurrency platform users and employees, including pages that impersonate Okta, iCloud, Gmail, Outlook, Yahoo, AOL, and Twitter.

The phishing operation was discovered by researchers at Lookout and more than 100 high-value victims of this campaign have been identified to date. Threat actors using the kit have been contacting users via SMS, email, and phone calls to trick them into visiting a malicious site where their credentials are harvested. Users are redirected to

a phishing site but before the content is displayed, they are required to pass an hCAPTCHA check. This helps with the credibility of the campaign, but most importantly it prevents automated analysis tools and security solutions from identifying the phishing site.

In the campaign targeting FCC employees, after passing the hCAPTCHA check, the user is presented with a login page that is a carbon copy of the FCC Okta page. The domain on which the page is hosted – fcc-okta[.com] – differs only slightly (1 character) from the legitimate FCC Okta login page. Login credentials alone are not normally enough to gain access to accounts as many are now protected by MFA. The captured login credentials are used to log in to the real account in real time, and the victim is then directed to the appropriate page where additional information is collected to pass the MFA checks. This could be a page that requests their SMS-based token or the MFA token from their authenticator app. Once the MFA check has been passed and the account has been accessed by the threat actor, the victim can be redirected anywhere. For instance, they could be shown a message that the login has been unsuccessful and they must try again later.

To target cryptocurrency platform users, messages are sent about security alerts such as warnings that their account has been accessed. These messages are likely to attract a rapid response due to the risk of substantial financial losses. In the campaign targeting Coinbase, the user is told they can secure their account and if they log in they can terminate suspicious devices. A similar process is used to obtain the credentials and MFA codes needed to access the account as the FCC campaign.

This is just one of many phishing kits offered on the dark web. Protecting against these phishing kits requires a combination of measures including an advanced spam filter, web filter, and security awareness training. For further information on cybersecurity solutions capable of combatting advanced phishing attempts, give the TitanHQ team a call.

State Sponsored Hackers and Cybercriminal Groups Are Using AI to Improve Their Campaigns

by G Hunt | February 29, 2024 | Network Security

There is growing evidence that cybercriminal groups are leveraging artificial intelligence in their cyberattacks, specifically large language models (LLMs) such as ChatGPT, despite the restrictions OpenAI has put in place. There are also LLMs that are being marketed directly to cybercriminals such as WormGPT. WormGPT is a blackhat AI tool that has been specifically developed for malicious uses and can perform similar tasks to ChatGPT but without any ethical restrictions on uses. The tool can be used for generating convincing phishing and business email compromise emails in perfect English, free from the spelling mistakes and grammatical errors that are often found in these emails.

It is not only cybercriminal groups that are using these AI tools. Nation state hacking groups are exploring how these tools can help them gain initial access to targeted networks. Recently published research from Microsoft and OpenAI confirmed that threat actors from Russia, China, Iran, and North Korea and using AI tools to support their malicious activities. Microsoft and OpenAI found the most common uses of LLMs by nation state actors were for translation, finding coding errors, running basic coding tasks, and querying open-source information. While it

does not appear that they are using LLMs to generate new methods of attack or write new malware variants, these tools are being used to improve and accelerate many aspects of their campaigns.

The threat actor tracked by Microsoft as Crimson Sandstorm, which is affiliated with the Islamic Revolutionary Guard Corps (IRGC), a multi-service primary branch of the Iranian Armed Forces, has been using LLMs to improve its phishing campaigns to gain initial access to victims' networks. Microsoft and OpenAI also report that the hacking group has been using LLMs to enhance its scripting techniques to help them evade detection. The North Korean APT group, Emerald Sleet, is well known for conducting spear phishing and social engineering campaigns and is using LLMs to assist with researching think tanks and key individuals that can be impersonated in its spear phishing campaigns. Threat groups linked to the People's Republic of China such as Charcoal Typhoon and Salmon Typhoon have been using LLMs to obtain information on high-profile individuals, regional geopolitics, US influence, and internal affairs and for generating content to socially engineer targets. OpenAI says it has terminated the accounts of five malicious state actors and has worked with Microsoft to disrupt their activities, and OpenAI and Microsoft have been sharing data with other AI service providers to allow them to take action to prevent malicious uses of their tools.

It should come as no surprise that cybercriminals and nation state actors are using AI to improve productivity and the effectiveness of their campaigns and are probing the capabilities of AI-based tools, and while this is a cause of concern, there are steps that businesses can take to avoid falling victim to AI-assisted attacks. The best way to combat AI-assisted attacks is to leverage AI for defensive purposes. SpamTitan has AI and machine learning capabilities that can detect zero day and AI-assisted phishing, spear phishing, and business email compromise attacks and better defend against AI-0assisted email campaigns.

With fewer spelling mistakes and grammatical errors in phishing emails, businesses need to ensure they provide their workforce with comprehensive training to help employees recognize email and web-based attacks. The SafeTitan security awareness training and phishing simulation platform is an ideal choice for conducting training and phishing simulations and improves resilience to a range of security threats. TitanHQ's data shows susceptibility to phishing attacks can be reduced by up to 80% through SafeTitan training and phishing simulations. Businesses should also ensure that all accounts are protected with multi-factor authentication, given the quality of the phishing content that can be generated by AI tools, and ensure that cybersecurity best practices are followed, and cybersecurity frameworks are adopted. The most important advice that we can give is to take action now and proactively improve your defenses, as malicious uses of AI are only likely to increase.

Phishing-as-a-Service Poses a Serious Threat to Businesses

by G Hunt | February 28, 2024 | Phishing & Email Spam

Cybercriminals are increasingly offering services that make it easy for anyone to conduct an attack. Skilled malware developers can concentrate on writing their malware and making it available for others to use for a fee, ransomware-as-a-service allows hackers who are skilled at breaching networks to conduct lucrative ransomware attacks without having to develop encryptors and pay for the infrastructure to their support attacks, and phishing-as-a-service provides a platform for conducting attacks to steal credentials and access accounts. These services benefit all parties and allow even more attacks to be conducted.

Phishing campaigns may appear simple, but they require a lot of time and skill to set up. Stephanie Carruthers, who leads an IBM X-Force phishing research project, said it takes her team about 16 hours to craft a phishing email, not including the time it takes to set up all the necessary infrastructure to send the email and steal credentials. Setting up the infrastructure is time-consuming and costly, and many businesses now have multi-factor authentication (MFA) to thwart attacks.

With phishing-as-a-service (PhaaS), anyone who wants to run a phishing campaign can simply pay a subscription and will be provided with all the tools they need to conduct attacks. They do not need to craft the phishing emails, they just need to set a few parameters and provide the email addresses for the campaign. PhaaS makes conducting sophisticated attacks simple and significantly lowers the bar for conducting campaigns.

Take LabHost, for example, a PhaaS platform that recently introduced functionality for targeting financial institutions and banks in North America and Canada. Since this new functionality was included in the first half of 2023, attacks have increased considerably. A monthly subscription is paid, and customers are provided with a turnkey phishing kit, which includes the infrastructure for hosting phishing pages, a content generator for creating phishing emails, and a portal for monitoring the progress of campaigns. Customers can choose to pay $179 per month to target Canadian banks, $249 per month to expand the targets to North America, and $300 a month to also target 70 financial institutions worldwide. Customers are also provided with phishing pages for collecting credentials or a variety of other companies, including music streaming sites, delivery services, and telecommunications companies.

Important to the success of any campaign is the ability to defeat multi-factor authentication. The LabHost phishing kit incorporates LabRat, a phishing tool that allows real-time management of phishing campaigns and allows adversary-in-the-middle attacks where two-factor authentication codes and cookies are obtained in addition to usernames and passwords. That means the additional security processes on the online portals of banks can be circumvented. The platform also allows SMS-based attacks to be conducted.

PhaaS allows unskilled hackers to conduct effective campaigns that they otherwise would not be able to conduct. Further, with the use of AI to craft convincing phishing emails, phishing emails are becoming much harder for humans and security solutions to detect, and even MFA and other security measures can be bypassed.

Defending against attacks is therefore challenging, and there is no single cybersecurity solution that will block all attacks. What is needed is a defense-in-depth approach, with multiple, overlapping layers of protection. Cybersecurity solutions are required to block the phishing emails. SpamTitan is an advanced email security solution with AI and machine learning capabilities for identifying novel phishing threats. SpamTitan blocks known malware through AV controls and unknown malware through sandboxing. The message sandboxing feature uses pattern filtering to identify malware from its behavior, which allows zero-day malware threats to be identified and blocked. Malware sandboxing is vital for email security since so many novel malware threats are now being released. SpamTitan is also capable of identifying even machine-crafted phishing content.

End user training is also vital, as no email security solution will block all email threats without also blocking an unacceptable number of genuine emails. End users should be trained on how to identify, avoid, and report phishing emails. The SafeTitan security awareness training platform makes security awareness training simple, and the constantly updated content allows businesses to respond to changing phishing tactics and conduct phishing simulations on the workforce to reinforce training and identify knowledge gaps.

Given the number of phishing kits that are capable of bypassing multi-factor authentication, simply enabling MFA on accounts is no longer sufficient to protect against unauthorized access. Phishing-resistant multi-factor authentication is required – FIDO/ WebAuthn authentication or Public key infrastructure (PKI)-based MFA – to block adversary-in-the-middle attacks that can be conducted through PhaaS.

If you want to improve your defenses against phishing and other cybercriminal services, give the TitanHQ team a call to discuss your options.

Massive Spamming Campaign Uses Thousands of Hijacked Subdomains

by G Hunt | February 26, 2024 | Phishing & Email Spam

A massive email spamming campaign has been detected that is generating up to 5 million emails per day that direct recipients of the emails to a variety of scam sites. The emails are sent through hijacked subdomains and domains of trusted companies, which help these emails evade email security solutions and be delivered to inboxes. Companies that have had domains and subdomains hijacked include eBay, CBS, McAfee, MSN, and Symantec.

Email security solutions perform a range of checks on inbound emails, including reputation checks on the senders of emails. If a domain is trusted and has not previously been associated with spamming, these checks – using SPK, DKIM, and DMARC – are likely to be passed, resulting in the emails being delivered to end users. The use of these legitimate domains also makes it harder for end users to determine whether the messages are genuine.

Security awareness training programs often teach end users to check the sender of the email and make sure that it matches the company being spoofed. If the domain is eBay, and the email uses eBay branding, end users are likely to think that the communication is genuine. These emails include links to websites that generate fraudulent ad revenue, and often several redirects occur before the user lands on the destination scam or phishing site.

The 'SubdoMailing' campaign was identified by researchers at Guardio Labs, with the legitimate domains typically hijacked through SPF record exploitation or CNAME hijacking. The former involves searching for domains that use the 'include' configuration option that points to external domains that are no longer registered. Those domains are then registered by the threat actor and the SPF records are changed to authorize the use of their own email servers. When those servers are used to send emails, they appear to have been sent by the targeted brand, such as eBay.

With CNAME hijacking, scans are conducted to identify subdomains of reputable brands with CNAME records that point to external domains that are no longer registered. The threat actor then registers those domains, SPF records are injected, and emails can be sent from their email servers to show that they have been sent by a legitimate company. By hijacking huge numbers of domains and subdomains, the threat actor is able to conduct massive spamming campaigns. The researchers identified more than 13,000 subdomains and more than 8,000 domains that were used in the campaign, with more than 1000 residential lines used and almost 22,000 unique IPs. The researchers developed a tool to allow domain owners to check whether their own domains have been hijacked and take action to stop that abuse. An advanced spam filter is required to block the messages that are set from these hijacked domains and subdomains – one that does not rely on SPF, DKIM, and DMARC for identifying spam emails.

Travel Companies Impersonated in Malware Distribution Campaign

by G Hunt | February 26, 2024 | Phishing & Email Spam

Cybercriminals are constantly devising new email campaigns for distributing malware. These campaigns usually impersonate a trusted entity and advise the email recipient about a pressing issue that requires immediate attention. The emails often have an attached file that must be opened to find out further information about the issue detailed in the email.

One recently detected campaign impersonates travel service providers such as booking.com and advises the recipient about a problem with a recent booking. One of the intercepted emails explains that an error has occurred with a booking that has resulted in a double charge to the user's credit card which requires immediate attention. The email has a PDF attachment which needs to be opened for further information. PDF files are increasingly being used in email campaigns for distributing malware. The PDF files often contain a script that generates an error message when the file is opened that tells the user that the content of the file cannot be displayed, and they are provided with an option to download the file.

In this campaign, the PDF file contains a script that generates a fake popup message. If clicked, a connection is made to a malicious URL and a download of an obfuscated JavaScript file is initiated. The script downloads the next stage PowerShell payload, and on execution, drops a malicious DLL file on the device. The DLL file searches for certain critical system processes and attempts to forcibly stop them, makes changes to the registry that affect

the Windows Antimalware Scan Interface (AMSI) and ensures that the malware is executed without being detected by security solutions. An analysis of the DLL file by researchers at Forcepoint shows the file is from the Agent Tesla malware family. Agent Tesla is a remote access trojan (RAT) that first appeared in 2014 and grew in popularity during the COVID-19 pandemic. Agent Tesla is provided under the malware-as-a-service model and is popular with initial access brokers, who specialize in gaining access to devices and accounts and then sell that access to other cybercriminals such as ransomware gangs.

Agent Tesla allows commands to be run on compromised systems and is capable of stealing sensitive information, such as login credentials stored in browsers. The malware can also take screenshots, log keystrokes, and perform other malicious actions. The malware uses multiple layers of obfuscation to ensure it is not detected by antivirus solutions. The malware is commonly used to gain initial access to business networks, primarily through phishing campaigns. In this campaign, by impersonating a popular travel service company there is a reasonable chance that the user may have used the service in the past or have a current booking and will therefore open the email. However, since the emails reference a charge to a credit card, that may be sufficient to get the user to open the attachment.

To protect against this and other malware distribution campaigns, businesses should ensure that they protect all endpoints with email security and antivirus solutions that are capable of behavioral analysis of files, as Agent Tesla and many other popular malware variants use obfuscation to bypass signature-based security solutions. Web filtering solutions provide added protection as they block connections to the malicious URLs that host malware and they can be configured to block downloads of executable files from the Internet. It is also important to provide security awareness training to the workforce to raise awareness of cyber threats and conduct phishing simulations to test the effectiveness of training.

TitanHQ offers a range of cybersecurity solutions for businesses and managed service providers to help them defend against cyber threats delivered via email and the Internet, including spam filtering with email sandboxing, web filtering, and security awareness training. Give the team a call today to find out more about improving your defenses against phishing and malware. All TitanHQ solutions are available on a free trial to allow you to test the products and see for yourself the difference they make.

Businesses Targeted with Phishing Emails Sent Via SendGrid

by G Hunt | February 23, 2024 | Email Scams

Small- and medium-sized businesses are being targeted in a phishing campaign that leverages the email service provider (ESP) SendGrid. SendGrid is a legitimate and well-known company that provides a customer communication platform for transactional and marketing email. SendGrid customer accounts are targeted to gain access to company mailing lists which can be used for a variety of email campaigns, such as phishing, spamming, and scams. In this campaign, the phishers compromise companies' SendGrid accounts and use the ESP itself to send phishing emails. Emails sent through the SendGrid platform are likely to be trusted by email security solutions, especially as the compromised accounts will have been used to send communications in the past. SendGrid may even be whitelisted to ensure that the emails are always delivered to inboxes. SendGrid emails are also likely to be trusted by end users.

In this campaign, the emails use a security-themed lure and inform the recipients that they need to set up 2-factor authentication – a perfectly reasonable request since 2-FA will better protect accounts against unauthorized access. The users are provided with a link that directs them to a malicious website that spoofs the SendGrid login, and if credentials are entered, they are harvested by the scammer. The emails were routinely delivered to inboxes and evaded email security solutions because the SendGrid was trusted.

SendGrid performs stringent checks on new accounts so it is difficult for malicious actors to use SendGrid directly, instead they compromise business SendGrid accounts, often through phishing attacks. Twilio SendGrid detected the malicious activity linked to customer accounts that were being used for phishing, and its fraud, compliance, and cyber security teams immediately shut down accounts. To better protect SendGrid accounts, users are advised to log in to their account and set up 2-factor authentication to prevent compromised credentials from granting access to user accounts.

The campaign demonstrates that even emails from reliable sources may not be what they seem. Many companies provide security awareness training to their employees that teaches cybersecurity best practices and trains employees on how to recognize and avoid phishing. It is important to include these types of emails in training material, as ESPs are being increasingly targeted by cybercriminals due to the effectiveness of campaigns run through an ESP.

With SafeTitan, keeping employees up to date on the latest tactics used by phishers and other cybercriminals is easy. The training content is regularly updated with new phishing templates based on real-world attacks and the latest phishing trends, and phishing simulations can be conducted on employees to test how they respond to phishing attempts outside of the training environment. SafeTitan is the only security awareness training platform that delivers targeted training automatically in response to bad security practices by employees, ensuring training is provided at the moment when it is most likely to be taken on board.

Massive Phishing Campaign Leverages Google Cloud Run to Deliver Banking Trojans

by G Hunt | February 22, 2024 | Phishing & Email Spam

A massive malware distribution campaign has been detected that uses phishing emails for initial contact with businesses and Google Cloud Run for hosting the malware. A variety of banking trojans are being distributed including Astaroth, Mekotio, and Ousaban. The campaign primarily targets countries in Latin America, and as such the majority of the phishing emails are in Spanish, but Italian versions have also been detected and there are indications that the campaign is spreading to other regions including Europe and North America.

The phishing emails used in this campaign appear to be legitimate invoices, statements, and communications from government and tax agencies and include a link that the recipient must click to view the attached invoice, statement, or demand. The link directs the user to services on Google Cloud Run, which is a popular service for hosting frontend and backend services and deploying websites and applications without having to manage infrastructure. Google Cloud Run has been used for hosting malware throughout 2023 but there was a massive spike in activity that started in September 2023 and has continued through January and February.

Over the past few months, Google's service has been proving popular with cybercriminals for hosting malware as it is both cost-effective and is generally not blocked by security solutions. If a user clicks the email link, an MSI file is downloaded onto their device. MSI files are executable files, which in this case include embedded JavaScript that downloads additional files and delivers one or more banking trojans.

The banking trojans achieve persistence through LNK files in the startup folder that execute a PowerShell command on boot that runs the infection script. The banking trojans are capable of keylogging, clipboard monitoring, screenshots, credential theft, and traffic manipulation to direct users to cloned websites of financial institutions to capture banking credentials. The Astaroth banking trojan alone targets more than 300 financial institutions as well as cryptocurrency exchanges.

To protect against this and other malware distribution campaigns, businesses need to adopt a defense-in-depth approach and should implement multiple layers of protection. The first line of defense is a spam filter or email security solution to block the initial phishing emails. SpamTitan Plus is a leading-edge anti-spam service that provides maximum protection against malicious emails. The solution has better coverage, faster phishing link detections, and the lowest false positive rate of any product, which makes it the best spam filter for businesses and an ideal MSP spam filtering solution In addition to including all leading phishing feeds to ensure the fastest possible detection of new phishing threats, SpamTitan Plus uses predictive analysis to identify suspicious URLs that have not yet been detected as malicious.

A web filter, such as WebTitan, can be used to control access to the Internet. For example, blocks can be placed on websites and certain categories of websites down to the user level, the solution prevents access to all known malicious URLs, and can be configured to block file downloads from the Internet, such as MSI files and other executable files that are often used for malware delivery.

Cybercriminals often host malware on legitimate hosting platforms which are usually trusted by security solutions, which means malicious emails may be delivered to end users. It is therefore important to provide security awareness training for the workforce. Security awareness training raises awareness of the threats that employees are likely to encounter and teaches them security best practices to help them identify, avoid, and report cyber threats. Combined with phishing simulations, it is possible to greatly reduce susceptibility to phishing and malspam emails. Data from companies that use the SafeTitan security awareness training platform and phishing simulator shows susceptibility to phishing threats can be reduced by up to 80%.

If you are looking to improve your defenses against phishing and malware, give the TitanHQ team a call to find out more about these products and to help get you set up for a free trial to put these solutions to the test in your own environment.

Malware Increasingly Distributed via Emailed PDF Files

by G Hunt | February 20, 2024 | Phishing & Email Spam

There has been a marked increase in email campaigns using malicious PDF files to distribute malware, rather than the typical uses of PDF files for obtaining sensitive information such as login credentials.

Increased security measures implemented by Microsoft have made it harder for cybercriminals to use macros in Office documents in their email campaigns, with PDF files a good alternative. Malicious links can be embedded in PDF files that drive victims to web pages where credentials are harvested. By using PDF files to house the links, they are less likely to be blocked by email security solutions.

Over the past few months, PDF files have been increasingly used to distribute malware. One of the currently active campaigns uses malicious emailed PDF files to infect users with DarkGate malware. DarkGate malware is offered under the malware-as-a-service model and provides cybercriminals with backdoor access to infected devices. In this campaign, emails are sent to targets that contain a PDF attachment that displays a fake image from Microsoft OneDrive that suggests there was a problem connecting which has prevented the content from being displayed. The user is given the option to download the PDF file; however, the downloaded files will install DarkGate malware.

In this campaign, clicking the link does not directly lead to the malware download, instead, the click routes through an ad network, so the final destination cannot be identified by checking the link of the download button. Further, since the ad network uses CAPTCHAs, the threat actors can make sure that the destination URL is not revealed to email security solutions. If the CAPTCHA is passed, the user will be redirected to the malicious URL where they can download the file. This is often a compressed file that contains a text file and a URL file, with the latter downloading and running JavaScript code which executes a PowerShell command that downloads and executes the malicious payload.

PDF files have been used in many other malware campaigns, including those that distribute the Ursnif banking Trojan and WikiLoader malware. Recent campaigns distributing these malware variants have used parcel delivery lures with PDF file attachments that contain a link that prompts the user to download a fake invoice. Instead of the invoice, a zip file is downloaded that contains a JavaScript file. If executed, the JavaScript file downloads an archive, extracts the contents, and executes the malware payload. Another campaign uses PDF files to install the Agent Tesla remote access trojan using Booking.com-related lures.

Not only do PDF files have a greater chance of evading email security solutions, they are also more trusted by end users than Office file attachments. Security awareness campaigns are often focused on training employees about the risks of phishing, such as clicking links in unsolicited emails and the risks of opening unsolicited office files. Malicious email campaigns using PDF files arouse less suspicion and end users are more likely to be tricked by these campaigns.

It is important for businesses to incorporate PDF files into their security awareness training and phishing simulation campaigns to better prepare employees for this growing threat. With SafeTitan, adding new content in response to the changing tactics, techniques, and procedures of threat actors is a quick and easy process. Get in touch with the TitanHQ team today to find out more about the SafeTitan security awareness training and phishing simulation platform and discover the difference the solution can make to your organization’s security posture.

Business Microsoft 365 Accounts Attacks Using Greatness Phishing Kit

by G Hunt | January 31, 2024 | Phishing & Email Spam

Phishing has long been the most common way that cybercriminals gain initial access to business networks. A successful attack allows a threat actor to steal credentials and gain a foothold in the network, providing access to sensitive data and giving them the access they need to conduct a range of nefarious actions. Phishers must develop campaigns that are capable of bypassing email security solutions and use lures that are likely to fool end users into disclosing their credentials or opening malicious email attachments. In recent years, the entry barrier for conducting phishing campaigns has been significantly lowered through phishing-as-a-service (PhaaS), which has proven popular with would-be cybercriminals.

Phishing kits are offered that provide everything needed to launch successful phishing campaigns, without having to spend hours setting up the infrastructure, creating convincing emails, and incorporating anti-detection measures to ensure emails land in inboxes. A relatively new phishing kit is proving to be particularly popular. The Greatness phishing kit has been available since mid-2022 and lowers the bar for starting phishing campaigns, requiring a payment of just $120 a month to use the kit. The Greatness phishing kit allows emails to be customized to suit the hacker's needs and add attachments, links, or QR codes to the emails. The kit makes it easy to generate and send emails and create obfuscated messages that can bypass many cybersecurity solutions and land in inboxes. The kit also supports multi-factor authentication (MFA) bypass by performing a man-in-the-middle attack to steal authentication codes and can be integrated with Telegram bots.

The kit has an attachment and link builder that creates convincing login pages for harvesting Microsoft 365 credentials and even pre-fills the victim's email address into the login box, only requiring them to enter their password. The kit also adds the targeted company's logo to the phishing page along with a background image that is extracted from the targeted organization's M365 login page. As such, the Greatness phishing kit is aimed at individuals looking to target businesses and can be easily purchased through the developer's Telegram channel. There were several spikes in Greatness phishing kit activity in 2023, with the latest detected in December 2023 and the increased activity has continued into 2024. Phishing kits such as Greatness significantly lower the barrier for entry to cybercrime and make it as easy as possible to start phishing, and the low cost of the kit has made it an attractive option for would-be cybercriminals. This phishing kit is used to target Microsoft 365 users, and the emails can be convincing and are likely to fool many end users.

The key to defending against phishing attacks is to implement layered defenses to ensure that a failure of one defensive measure does not leave the business unprotected. TitanHQ has developed a suite of cybersecurity solutions for businesses and the MSPs that serve them to improve their defenses against phishing, including AI-generated phishing emails and sophisticated phishing kits capable of stealing passwords and MFA codes.

TitanHQ's PhishTitan provides advanced phishing protection and remediation for Microsoft 365. TitanHQ's proprietary machine-learning algorithm integrates directly with Microsoft 365 and catches and remediates sophisticated phishing including AI-generated phishing emails, business email compromise, spear phishing, and phishing attacks that bypass MFA. The solution augments rather than replaces EOP and Defender and catches the phishing attempts that those defensive measures often miss.

PhishTitan uses AI and a large language model (LLM) with proprietary threat intelligence currently not found in any other anti-phishing solution on the market, and will scan attachments for malicious links and malware, rewrite URLs, apply banner notifications, and block malicious links. PhishTitna also provides time-of-click protection to combat the weaponization of links after delivery. The solution uses machine learning algorithms to scan the

message body to assess email content and identify words, phrasing, and formatting of emails indicating a phishing attempt, and will learn over time and become even more effective.

PhishTitan is suitable for businesses of all types and sizes and has been developed from the ground up to meet the needs of MSPs. The solution can be set up in less than 10 minutes, and MSPs can add new clients in less than 6 minutes and start protecting them from highly sophisticated phishing attacks. For maximum protection, TitanHQ also offers WebTitan DNS filter to protect against web-based attacks, ArcTitan email archiving for security and compliance, EncryptTitan for email encryption, SafeTitan for security awareness training and phishing simulations, and the SpamTitan Suite of email security solutions. All products are available on a no-obligation, 100% free trial and product demonstrations are available on request. For more information on PhishTitan and other TitanHQ solutions, give the TitanHQ team a call today.

TitanHQ Launches PhishTitan – AI-Driven Phishing Protection for M365

by G Hunt | January 14, 2024 | Industry News, Phishing & Email Spam

TitanHQ is proud to announce the addition of a new solution to its cybersecurity portfolio that helps businesses combat the growing threat of phishing. PhishTitan provides powerful phishing protection for Microsoft 365 that is capable of catching and remediating sophisticated phishing attempts, including spear phishing attacks, business email compromise, phishing emails generated by artificial intelligence tools, and zero-day phishing threats that Microsoft's native defenses for M365 fail to detect and block. It is these threats that pose the biggest threat since they are missed by Microsoft's email security defenses and are difficult for employees to identify as malicious since they lack many of the red flags that employees are taught to look out for in security awareness training programs.

PhishTitan incorporates TitanHQ's proprietary machine-learning algorithm, which integrates directly with M365. PhishTitan performs an AI-driven analysis of inbound emails (internal and external) which includes textual analysis, link analysis, and attachment scanning. Links are analyzed via multiple curated feeds that constantly update the solution to allow malicious websites linked to phishing and malware distribution to be identified and blocked. Phishing emails often include links that have been masked to hide the true destination URL. PhishTitan rewrites URLs to show the true destination. One tactic used by phishers to bypass email security solutions is to only weaponize links in emails after delivery. To protect against this tactic, PhishTitan checks inbound emails before delivery to inboxes and also offers time-of-click protection against malicious links in emails.

Attachments are scanned with twin antivirus engines, and suspicious email attachments are sent to the sandbox for behavioral analysis. Machine learning detection models scour the body of emails looking for tell-tale signs of phishing and adapt to constantly changing phishing tactics. The machine learning algorithms also learn from reports of phishing attempts by end users, which they can report with a single click using a TitanHQ-supplied Outlook add-in. PhishTitan can also be configured to apply banner notifications to external emails and protect against the leakage of sensitive company information.

The solution has been designed to meet the needs of businesses of all types and sizes and has been developed from the ground up to meet the needs of managed service providers (MSPs) to allow them to easily add advanced

phishing protection to their service stacks. It takes around 10 minutes to set up the solution, and around 6 minutes for MSPs to onboard new clients.

The solution was trialed across the TitanHQ user database of more 12,000 customers and 3,000 MSPs in Q4, 2023, with TitanHQ customers reporting that the solution outperforms their existing anti-phishing solutions. TitanHQ is now pleased to start offering the new product to new customers. For more information on PhishTitan phishing protection Microsoft 365 contact TitanHQ today. PhishTitan is available on a 14-day free trial and product demonstrations can be arranged on request to show you how easy the product is to use and exactly what it can do.

“A staggering 71% of MS business users suffer at least one compromised account monthly. With this in mind, the overwhelming feedback from our customer base has been that phishing is the number one problem to solve in the email security community,” said TitanHQ CEO, Ronan Kavanagh. “We therefore allocated resources and investment to develop a solution with new, cutting-edge, robust, fast phishing threat intelligence driven by a team of security specialists. We are pleased to be able to meet the market’s needs with a product that delivers.”

Advantages and Disadvantages of Email Sandboxing

by G Hunt | November 10, 2023 | Network Security, Spam Software

Sandboxing is the use of a virtual environment for testing code and safely opening untrusted files. The sandbox is an isolated and secure environment that emulates a legitimate endpoint; however, there are no connections to the business network, the sandbox environment contains no real data, and if dangerous code is executed, no harm will be caused.

Advantages of Email Sandboxing

Sandboxing is important because of the sheer number and complexity of threats faced by businesses. Cybercriminal groups are conducting increasing numbers of attacks, new groups are constantly being formed, and their attacks are becoming much more sophisticated. The cost of these attacks and the resultant data breaches are also spiraling. According to the 2023 Cost of a Data Breach Report from IBM, on average, data breaches cost $4.45 million to resolve in the United States and $10.93 million for a healthcare data breach.

Many of these threats come from email. Emails are used to send attachments containing malicious code that downloads malware that provides a cyber actor with access to the network. Links to malicious websites are also distributed via email where malware is downloaded. While businesses have a degree of protection if they have anti-virus software installed, most anti-virus solutions can only detect known malware variants – Malware that has previously been analyzed and had its signature added to the solution’s malware definition list. Antivirus solutions will not detect new malware variants nor fileless malware, which is executed in the memory with no files downloaded to the disk.

Sandboxing provides an additional layer of protection against zero-day malware and ransomware attacks and will allow malicious files to be identified, detected, and quarantined before they can do any harm, even if they have not previously been encountered. In the sandbox, malware is identified by the actions it tries to perform, not by any signature.

Disadvantages of Email Sandboxing

While there are clear benefits, there are some disadvantages of email sandboxing. Businesses may want to add email sandboxing to their cybersecurity arsenal, but email sandboxes can be complicated to set up and run, and they can require a considerable amount of resources and can be expensive to run. Another of the disadvantages of email sandboxing is analyzing file attachments takes time and messages cannot be delivered until all checks have been performed. It is therefore inevitable that there will be email delivery delays.

As with any cybersecurity solution, there is the potential for false positives. An email attachment may be determined to be malicious when it is actually harmless. In such cases, important business emails may be blocked or deleted. The last main disadvantage is malware often contains code that determines if it has landed on the targeted endpoint or if it is in a virtual environment. If the latter is detected, the malware may delete itself or not perform any of its programmed malicious actions. Considering the cost of a successful cyberattack, the advantages of email sandboxing outweigh the disadvantages, provided the right sandboxing solution is chosen.

SpamTitan Email Security with Sandboxing

SpamTitan is an award-winning email security solution from TitanHQ that provides advanced threat protection at an affordable price. The solution is easy to implement and use and protects thousands of SMBs and managed service providers (MSPs) by blocking spam, viruses, malware, ransomware, and links to malicious websites from your emails. SpamTitan's ATP defense uses inbuilt Bayesian auto-learning and heuristics to defend against advanced threats and evolving cyberattack techniques and features an integrated email sandbox tool that is part of Bitdefender's Global Protective Network.

SpamTitan uses advanced intelligent technologies, such as AI, to predict and prevent advanced threats and the sandbox accurately mimics a real endpoint to trick malware into determining it has reached its intended target. As with any sandbox, there are delays in delivering emails but this is kept to a minimum. SpamTitan has multiple layers of security and sophisticated sandbox technology, which means only specific and dangerous emails will be sandboxed. Even if a legitimate email lands in a sandbox, the delivery delay will be, at most, twenty minutes. While there may be false positives on occasion, no emails are deleted. They are quarantined to allow administrators to check the validity of the results.

If you want to improve security and get the advantages of email sandboxes while eliminating the disadvantages, give the TitanHQ team a call today. SpamTitan is also available on a free 14-day trial to allow you to test the product and sandbox in your own environment before making a purchase decision.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing Pattern Filtering

Malicious File Sandbox for Email

by G Hunt | November 5, 2023 | Network Security, Spam Software

Multiple layers of security are required to protect against increasingly sophisticated email attacks. A malicious file sandbox for email should be one of those layers to ensure your business is protected against zero-day and stealthy malware threats.

Email: The Most Common Initial Access Vector Used by Cybercriminals

There are many ways that cybercriminals can attack businesses, but email is the most common initial access vector. Most employees have email accounts which means they can be easily reached, and social engineering techniques are used to trick employees into opening malicious attachments or visiting links in emails. Cybercriminals have become adept at exploiting human weaknesses in defenses.

One of the main aims of email campaigns is to deliver malware to provide persistent access to victims' networks. Executable files may be attached to emails and hidden using double file extensions to make the files appear to be legitimate documents, PDF files, or spreadsheets. Office files may be attached that have malicious macros which, if allowed to run, trigger the download of a first-stage malware payload. The problem for businesses is these campaigns are becoming much more sophisticated, they often bypass standard email security defenses, and they land in inboxes where they can be opened by employees.

Defending against sophisticated email attacks requires a defense-in-depth approach, which should include a spam filter/secure email gateway, a web filter, multifactor authentication, an endpoint detection and response solution,

and security awareness training for employees. To improve protection further and defend against new and stealthy malware threats, it is important to have a malicious file sandbox for email.

What is a Malicious File Sandbox?

A malicious file sandbox is an isolated virtual environment where untrusted, suspicious files can be detonated securely without risking network or data security. The sandbox is used for analyzing emails, documents, application files, and other executable files to determine their true nature. When an email is received, it must first pass through a spam filter which looks for the common signatures of spam and phishing emails, performs reputation checks on the sender, analyzes the message content, and scans email attachments using antivirus software. The spam filter will filter out the majority of spam and phishing emails and all known malware variants using the antivirus software.

The problem is many email attacks are stealthy and have been developed to be undetectable, and cyber actors are skilled at getting their emails past email defenses and into inboxes. One way this is achieved is by using polymorphic malware, which cannot be detected by standard email security solutions and antivirus software. A malicious file sandbox is needed to protect against these novel threats.

When suspicious files are received that pass the front-end checks, they are sent to the sandbox for in-depth analysis of their behavior. The malicious file sandbox is configured to look like a real target environment to ensure that when an email is sent to the sandbox any malware acts as it would in the wild and is tricked into determining that it has landed on the endpoint of its intended target. No harm can be caused in the sandbox as the environment is isolated and not set up locally. If malware is detected, a report is generated of any malicious intent or unexpected actions, and actionable insights are provided to allow the threat to be blocked.

The SpamTitan Malicious File Sandboxing Service

SpamTitan is an award-winning anti-spam and anti-phishing solution from TitanHQ that is used by thousands of businesses and managed service providers to protect against email-based attacks. The solution leverages artificial intelligence and machine learning algorithms to detect novel threats and predict new attacks, reputation checks are conducted using SPF, DKIM, and DMARC, users are protected from malicious links in emails, and the solution has dual antivirus engines that scan for known malware.

SpamTitan also includes a Bitdefender-powered malicious file sandbox for blocking zero-day malware threats. The sandbox analyzes a broad range of targets, including emails, documents, application files, and other executable files, and leverages purpose-built, advanced machine-learning algorithms, aggressive behavior analysis, anti-evasion techniques, and memory snapshot comparison to detect sophisticated threats and delivers advanced threat protection and zero-day exploit detection. The sandbox also extracts, analyzes, and validates URLs within files.

The sandbox is not located on the endpoint so there are no performance implications, and strong machine learning and behavior detection technologies ensure that only files that require further analysis are sent to the Sandbox. If a malicious file is detected, the sandbox informs Bitdefender’s cloud threat intelligence service to ensure the threat is instantly blocked globally and will not need to be set to the sandbox for analysis again. The sandbox allows

businesses to identify and block malicious files such as polymorphic malware and other threats that have been developed for use in undetectable attacks.

The SpamTitan malicious file sandbox delivers best-in-class detection, advanced anti-evasion technologies, innovative pre-filtering, and MITRE ATT&CK framework support. If you want the best protection from dangerous malware, you need a malicious file sandbox for email, and with SpamTitan you get that and more at a very affordable price. For more information on the capabilities of SpamTitan and details of pricing, give the TitanHQ team a call. SpamTitan is also available on a free 14-day trial to allow you to test the product in your own environment before making a purchasing decision.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing Pattern Filtering

How does an email sandbox block malware?

Email Sandboxing and Message Delivery Delays

Commonly Asked Questions about Email Sandboxing

What is sandbox security?

How does a sandbox work?

How to sandbox email attachments

What is message sandboxing?

What is malware sandboxing for email?

What is sandboxing in cybersecurity?

What are the advantages and disadvantages of email sandboxing?

Sandboxing Technology for Email

What is a malicious file sandbox for email?

What is Message Sandboxing?

by G Hunt | October 28, 2023 | Spam Advice, Spam Software

Message sandboxing is a security feature of spam filters, secure email gateways, and other email security solutions where inbound messages are sent to a secure and isolated environment where the messages are subjected to behavioral analysis. File attachments are detonated and analyzed for malicious properties and actions, such as attempted file downloads from the Internet, command-and-control center callbacks, and attempts to write code to the memory.

What is a Sandbox?

In the technology sense, a sandbox is a contained virtual environment that is separate and isolated from other applications, operating systems, data, and internal networks. Sandboxes have several uses. In software development, a sandbox is used for testing new code, where it can be observed for unexpected compatibility issues, allowing software developers to troubleshoot the code without causing any harm to live systems and data.

In cybersecurity, a sandbox is used to open untrusted files, follow potentially malicious links, and analyze suspicious code and malware. If malware was installed and executed on a standard machine, the threat actor would be given remote access, malware may exfiltrate sensitive data, or in the case of ransomware, encrypt files. Since the sandbox is a secure environment, any malicious action has no consequences, and files can be studied in safety.

A sandbox is a virtual environment that is often configured to mimic a genuine endpoint. One of the first actions taken by malware is to explore the environment it is in to check whether it is on a genuine device. If not, it is likely not to run any malicious routines and may self-delete to prevent analysis. By configuring the sandbox to mirror a genuine endpoint, the malware can be tricked into performing its malicious routines, which are detected and logged. The intelligence gathered is fed into the email security solution, and all users of that solution, locally and globally, will be protected from that malware sample in the future.

Why is Message Sandboxing Necessary?

Traditional email security solutions check message headers, perform reputation checks of senders, scan email attachments with antivirus engines, follow embedded hyperlinks, and examine the content of the message for known spam and phishing signatures. For many years, these checks alone have been sufficient and ensure that more than 99% of spam and phishing emails are detected and blocked along with all known malware.

Email attacks have been getting much more sophisticated in recent years and new malware variants are being released at never-before-seen rates. A malware phishing campaign, for instance, will not just use one iteration of malware, but many, with each sample differing sufficiently to defeat signature-based detection mechanisms. Cybercriminals are using automation to spin up masses of samples and AI is being used to develop novel phishing methods.

AI and machine learning capabilities are now required in email security for blocking these zero-day threats, and email message sandboxing is necessary for detecting novel malware threats. Advanced email security solutions leverage AI, machine learning, and email sandboxing and protect against the rapidly evolving threat landscape. Without these features, many malicious messages will be delivered.

How to Set Up Message Sandboxing

The easiest way to get started and set up message sandboxing is to use SpamTitan Email Security. SpamTitan has been developed to be easy to set up and use by businesses of all sizes, from small offices and coffee shops to small and medium-sized businesses and large enterprises. Being cloud-based, there is no software to install, just a small configuration change to your MX record (information on how to do this is provided). The solution can be accessed through a web-based interface, and the solution can be configured in just a few minutes.

Users benefit from spam and phishing detection rates of more than 99.99%, a very low false positive rate and a Bitdefender-powered email sandbox. The email sandbox leverages advanced machine learning algorithms, aggressive behavior analysis, anti-evasion techniques, and memory snapshot comparison to detect zero-day threats.

Without an email sandbox, you are likely to be exposed to many malicious messages. With sandbox email protection, you have much better control of the content that reaches user inboxes.

How to Sandbox Email Attachments

by G Hunt | October 15, 2023 | Phishing & Email Spam, Spam Software

Do you know how to sandbox email attachments? If you have yet to start using a sandbox for email, you will be exposed to advanced malware and phishing threats. The good news is it is quick and easy to improve protection with a sandbox, and it requires no advanced techniques or skills, but before presenting an easy email sandboxing solution, we should explain why email sandboxing is now a vital part of email security

Email Sandboxing Detects Advanced and Sophisticated Threats

A hacker writes the code for a new malware variant or generates the code using an AI tool, and then sends that malware via email. A traditional email security solution will not block that malware, as it has not detected it before and it doesn’t have the malware signature in its definition list. The email would most likely be delivered, and the intended recipient could open it and infect their device with malware. From there, the entire network could be compromised and ransomware could be deployed.

How could a new, previously unseen threat be blocked? The answer is email sandboxing. When a file passes initial checks, such as AV scans, the attachment is sent to an email sandbox where its behavior is analyzed. It doesn’t matter if the malware has not been seen before. If the file performs any malicious actions, they will be detected, the threat will be blocked, and if that threat is encountered again, it will be immediately neutralized.

Email sandboxing is now an essential part of email security due to the sheer number of novel malware variants now being released. That includes brand new malware samples, malware with obfuscated code, polymorphic malware, and known malware samples that differ just enough to avoid signature-based detection mechanisms. Without behavioral analysis in a sandbox, these threats will be delivered.

The Easy Way to Sandbox Email Attachments

Setting up an email sandbox need not be complicated and time-consuming. All you need to do is sign up for an advanced cloud-based email security solution such as SpamTitan Email Security. SpamTitan is a 100% cloud-based email security solution that requires no software downloads or complex configurations. Just point your MX record to the SpamTitan Cloud and use your login credentials to access the web-based interface. You can adjust the settings to suit your needs, and the setup process is quick, easy, and intuitive, and generally takes around 20-30 minutes.

The solution is fed threat intelligence from a global network of more than 500 million endpoints, ensuring it is kept up to date and can block all known and emerging threats. You will be immediately protected from known malware and ransomware threats, phishing emails, spam, BEC attacks, and spear phishing, and you will benefit from email sandboxing, where suspicious emails are sent for deep analysis to identify zero-day phishing and malware threats.

The SpamTitan email sandbox is powered by Bitdefender and has purpose-built, advanced machine learning algorithms, decoys and anti-evasion techniques, anti-exploit, and aggressive behavior analysis. If a file is analyzed in the sandbox and found to be malicious, SpamTitan updates Bitdefender's Global Protective Network, ensuring that the new threat is blocked globally.

Email sandboxing doesn't need to be complicated. Just use SpamTitan from TitanHQ. SpamTitan is available on a free trial, with customer support provided throughout the 14-day trial to help you get the most out of the solution. We are sure you will love it for the level of protection provided and how easy it is to use.

How Does a Sandbox Work?

by G Hunt | October 5, 2023 | Phishing & Email Spam, Spam Software

Sandboxing is a security feature that protects against malicious code. Rather than execute potentially unsafe code in a standard environment, it is sent to the sandbox – an isolated environment where no harm can be caused.

How Does a Sandbox Work?

A sandbox is an important cybersecurity tool for protecting host devices, operating systems, and data from being exposed to potential threats. The sandbox is a highly controlled system that is used to analyze untrusted applications, files, or code. The sandbox is isolated from the network and real data, and there are only essential resources that are authorized for use. It is not possible for a sandboxed file to access other parts of the network, resources, or the file system, only those specifically set up for the sandbox.

Sandboxes can have different environments. One of the most common implementations uses virtualization. A virtual machine (VM) is set up specifically to examine suspicious programs and code. Some sandboxes include emulation of operating systems to mimic a standard endpoint. Some malware samples perform checks of their environment before executing malicious routines to make sure they are not in a VM. If a VM is detected, the malware will not execute malicious routes and may self-delete to prevent analysis. By emulating a standard endpoint, these checks can be passed to allow analysis. Some sandboxes have full system emulation, which includes the host machine's physical hardware as well as its operating system and software. These sandboxes provide deeper visibility into the behavior and impact of a program.

In email security, files, attachments, URLs, and programs are sent to the sandbox to check whether they are benign or malicious. The analyses can take between a few seconds to a few minutes, and if any malicious activity is detected, the file will be either quarantined and made available for further study or it will be deleted. Any other instances of that file will be removed from the email system, and any future encounters will see the file, attachment, URL, or program deleted.

SpamTitan Email Sandboxing

SpamTitan Email Security includes a Bitdefender-powered email sandbox to ensure users are protected against zero-day threats. All emails are subjected to a barrage of checks and tests, including scans using two different antivirus engines. SpamTitan features strong machine learning, static analysis, and behavior detection technologies to ensure that only files that require deep analysis get sent to the sandbox. This is important, as deeper analysis may take several minutes, so verified clean and safe messages will not be unduly delayed.

Files that are sent to the sandbox for deep analysis are executed and monitored for signs of malicious activity, with self-protection mechanisms in place to ensure every evasion attempt by a piece of malware is properly marked. The sandbox has purpose-built, advanced machine learning algorithms, decoys and anti-evasion techniques, anti-exploit, and aggressive behavior analysis. All results are checked across known threats in an extensive array of online repositories. If a malicious file is detected, the sandbox updates the Bitdefender's cloud threat intelligence service – the Bitdefender Global Protective Network – and the sandbox will never have to analyze that threat again as it will be blocked globally.

If you want to improve protection against zero-day threats, give the TitanHQ team a call to find out more about SpamTitan. SpamTitan is available on a free trial to allow you to test it out in your own environment before making a purchase decision.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing Pattern Filtering

How does an email sandbox block malware?

Email Sandboxing and Message Delivery Delays

Commonly Asked Questions about Email Sandboxing

What is sandbox security?

How does a sandbox work?

How to sandbox email attachments

What is message sandboxing?

What is malware sandboxing for email?

What is sandboxing in cybersecurity?

What are the advantages and disadvantages of email sandboxing?

Sandboxing Technology for Email

What is a malicious file sandbox for email?

Email Sandboxing is the Key to Blocking More Malware Threats

by G Hunt | September 27, 2023 | Phishing & Email Spam, Spam Software

https://www.spamtitan.com/blog/email-sandboxing-key-blocking-malware-threats/Email security solutions with email sandboxing block more malware threats than traditional spam filters, even novel malware variants that have yet to be identified as malicious. Without this important feature, emails with malicious attachments will likely be delivered to inboxes where they can be opened by employees. All it takes is for one employee to open a malicious file for malware to be installed that gives a threat actor the foothold they need for a comprehensive attack on the network.

What is an Email Sandbox?

In cybersecurity terms, a sandbox is an isolated, virtual machine where potentially unsafe code can be executed in safety, files can be subjected to deep analysis, and URLs can be visited without risk. In the sandbox, the behavior of files, code, and URLs is inspected, and since the sandbox is not networked and there is no access to real data or applications, there is no risk of causing any damage. Email sandboxing is used to identify malicious code and URLs in emails. The email sandbox mirrors standard endpoints to trick malicious actors into thinking that they have reached their intended target. Emails may pass front-end tests that look at the reputation of the sender, email headers, the content of the messages, and subject attachments to signature-based anti-virus tests, but there is no guarantee that the emails are safe without sandbox-based behavioral analysis.

Why is Email Sandboxing Important?

Cyber threat actors have been developing techniques for bypassing standard email security solutions such as embedding malicious URLs in PDF attachments, hiding malicious content in compressed files, using multiple redirects on hyperlinks, and including links to legitimate cloud-based platforms such as SharePoint for distributing malware. Traditional email security solutions can filter out spam and phishing emails, but they often fail to block more sophisticated threats, especially zero-day malware threats. Email sandboxing provides an extra layer of protection against sophisticated threats such as spear-phishing emails, advanced persistent threats (APTs), and novel malware variants.

A few years ago, new malware variants were released at a fairly slow pace; however, threat actors are now using automation and artificial intelligence to generate new malware variants at an alarming rate. Malware samples are

used that deviate sufficiently from a known threat to be able to bypass signature-based detection mechanisms, ensuring they reach their intended targets. Rather than just using one version of malware in their email campaigns, dozens of versions are created on a daily basis. While security awareness training will help employees identify and avoid suspicious emails, threat actors have become adept at social engineering and often hoodwink employees.

The SpamTitan Email Sandbox

The SpamTitan email sandbox is a powerful next-generation security feature with award-winning machine-learning and behavioral analysis technologies. Powered by Bitdefender, the SpamTitan sandbox for email allows files to be safely detonated where they can do no harm. Email attachments that pass the barrage of checks performed by SpamTitan are sent to the sandbox for deep analysis. The sandbox is a virtual environment that is configured to appear to be a typical endpoint and incorporates purpose-built, advanced machine learning algorithms, decoys and anti-evasion techniques, anti-exploit, and aggressive behavior analysis. Files are also subjected to checks across an extensive array of online repositories, with the sandbox checks taking just a few minutes. That ensures that genuine emails are not unduly delayed. If malicious properties are detected in the sandbox, the threat intelligence is passed to Bitdefender's Global Protective Network (cloud threat intelligence service). If the threat is encountered again, it will be detected and blocked without having to be analyzed again in the sandbox.

The SpamTitan sandbox is used for a wide range of attachments, including office documents to check for malicious URLs, macros, and scripts, and all executable and application files. The sandbox allows SpamTitan to detect polymorphic malware and other threats that have been designed for use in undetectable targeted attacks. If a malicious file is detected, the email is not sent to a spam folder where it could be opened by an end user, it is quarantined in a directory on the local email server which only an administrator can access. Administrators may wish to conduct further investigations to gain insights into how their organization is being targeted.

Threat actors are conducting increasingly sophisticated attacks, so email security solutions need to be deployed that are capable of detecting these advanced threats. With zero-day threats on the rise, now is the ideal time to improve your email defenses with SpamTitan. Why not sign up for a free trial of SpamTitan today to put the solution to the test to see the difference the advanced threat detection capabilities make to your security posture? Product demonstrations can also be requested by contacting TitanHQ, and our friendly sales team will be more than happy to discuss SpamTitan with you and the best deployment options to meet the needs of your business.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing Pattern Filtering

How does an email sandbox block malware?

Email Sandboxing and Message Delivery Delays

Commonly Asked Questions About Email Sandboxing

by G Hunt | September 15, 2023 | Phishing & Email Spam, Spam Software

Commonly asked questions about email sandboxing so you know what to expect from an email security solution with a sandbox, and why this advanced feature is vital for email security.

What is an Email Sandbox?

One of the commonly asked questions about email sandboxing is what is an email sandbox? Like the children's equivalent, it is a safe space for building, destroying, and experimenting. In cybersecurity terms, it is an isolated environment where harm cannot be caused to anything outside of that environment. An email sandbox is an isolated virtual machine that is used for performing risky actions, such as opening unknown attachments and analyzing files and URLs in depth, rather than using a real machine where there is a risk of harm being caused such as file encryption by ransomware, theft of sensitive information, or wiping of data.

Why is an Email Sandbox Important?

Email is the most common vector used in cyberattacks. Through emails, cyber threat actors can gain initial access to a protected network from where they can steal sensitive data or move laterally for a more comprehensive attack. One of the most common ways of gaining remote access is through malware. Once malware is downloaded, an attacker can remotely perform commands and gain full control of an infected device. While businesses use antivirus software to detect and remove malware, these solutions are signature-based. In order to detect malware, the signature of the malware must be in the definition list used by the anti-virus solution, which means the malware must have previously been encountered. Novel malware variants that have not yet been determined to be malicious will not be identified as such and will therefore be delivered to inboxes where they can be executed by employees. An email sandbox is used to safely detonate suspicious files and inspect their behaviors. The

behavioral analysis allows previously unknown malware samples can be identified and blocked. This is important due to the volume of new malware samples that are now being released.

How Does an Email Sandbox Protect Against Malware?

Email security solutions with sandboxing perform the same front-end checks as traditional email security solutions and will identify and block many malicious messages. If the initial checks are passed, and the messages are determined to potentially pose a risk, they will be sent to the sandbox for behavioral analysis. Once inside the safety of the sandbox, the attachments will be opened and subjected to various tests. The sandbox is configured to appear to be a normal endpoint, so any malware will be tricked into running malicious commands as it would if it had reached its intended target. The actions of the file are assessed, and if they are determined to be malicious they will be sent to a quarantine folder. By performing these checks, new malware variants can be identified and blocked before any harm is caused.

Will Sandboxing Delay Message Delivery?

Performing standard checks of messages is a quick process, often causing imperceptible delays in mail delivery. Performing in-depth analysis takes longer, so there will be a delay in message delivery. Many emails will not need to be sent to the sandbox and will be delivered immediately, but if sandboxing is required, there will be a delay while the behaviors of the email and attachments are analyzed. Some malware has built-in anti-analysis capabilities and will delay any malicious processes to combat sandboxing. Time is therefore required to ensure full analysis. With SpamTitan, the delay will be no longer than 20 minutes.

How Can I Avoid Message Delivery Delays?

SpamTitan incorporates artificial intelligence and machine learning capabilities which minimize the number of emails that are sent to the sandbox, and SpamTitan will check every 15 seconds to ensure that emails are delivered as soon as the sandbox analysis is complete. SpamTitan's sandbox is part of Bitdefender's Global Protective Network, which ensures rapid checks of suspicious messages. To avoid delays, certain email addresses and domains can be added to a whitelist, which means they will not be sent to the sandbox for analysis, ensuring rapid delivery.

What are the Benefits of Email Sandboxing?

The sandbox provides an important extra layer of protection against malware threats and malicious links. It will detect advanced attacks early and prevent breaches, reduce incident response costs and efforts, reduce the threat-hunting burden, and increase the detection rate of elusive threats in the pre-execution stage, including APTs, targeted attacks, evasion techniques, obfuscated malware, custom malware, ransomware.

How Does the SpamTitan Sandbox Work?

SpamTitan will subject all inbound emails to a battery of front-end tests, and if these are passed but the email is still suspicious, the message and attachment will be sent to the sandbox and the user will be informed that the message is in the sandbox for review. The email and attachments will then be opened in an isolated cloud platform

or a secure customer virtual environment. If malware is detected, the email is blocked and assigned ATP.Sandbox and will be listed under “Viruses” in the relevant quarantine report and the intelligence gathered will be used to protect all users from that threat in the future. After twenty minutes of interrogation, if no malicious actions are identified, the file is marked clean and the email is passed onto the recipient.

How Can I Find Out More About Email Security and Sandboxing?

If you have unacceptable numbers of spam and malicious messages being delivered to inboxes, are receiving large numbers of queries about suspicious emails from your employees, or if you have experienced a malware infection via email recently, you should speak with TitanHQ about improving email security with SpamTitan.

SpamTitan has artificial intelligence and machine learning capabilities, a next-gen email sandbox, and a 99.99% detection rate with a very low false positive rate. Further, SpamTitan is very competitively priced, easy to use, and requires little maintenance. The solution is also available on a 100% free trial, with full product support provided for the duration of the trial.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing Pattern Filtering

How does an email sandbox block malware?

Email Sandboxing and Message Delivery Delays

Commonly Asked Questions about Email Sandboxing

What is sandbox security?

How does a sandbox work?

How to sandbox email attachments

What is message sandboxing?

What is malware sandboxing for email?

What is sandboxing in cybersecurity?

What are the advantages and disadvantages of email sandboxing?

Sandboxing Technology for Email

What is a malicious file sandbox for email?

TitanHQ Announces New Partnership with India's Leading Managed Service Provider

by G Hunt | September 13, 2023 | Industry News

TitanHQ has recently announced a new partnership with one of India's leading managed service providers, Tata Tele Business Services (TTBS). TTBS is the leading provider of business connectivity and communications solutions in India and has the largest portfolio of ICT services for businesses in the country.

Like many countries, India is facing a major increase in cybercrime. 78% of Indian organizations experienced a ransomware attack in 2021, web-based attacks have jumped sharply, and a 2022 Group-IB study placed India third globally for phishing attacks in 2021 with more attacks than any other country in the Asia-Pacific region. Indian businesses need to ensure that they have the necessary defenses in place to combat increasingly sophisticated cyberattacks, especially attacks that target employees.

Businesses often turn to their managed service providers for cybersecurity and seek solutions that can protect them against malware and phishing. TTBS provides cybersecurity solutions to SMBs and its cybersecurity packages have now been improved with the addition of SpamTitan email security and the WebTitan DNS-based web filter. Both solutions are 100% cloud-based, easy for MSPs to add to their service stacks, and easy to manage.

TTBS provides advanced email security with phishing protection through the Tata Tele Email Security Plus Program, which delivers advanced threat protection for email through TitanHQ's AI-driven SpamTitan anti-phishing solution. Protection against Internet-based threats is provided through the Tata Tele Smart Internet Program, which includes web filtering provided by WebTitan. WebTitan is fed threat intelligence from a network of 650 million endpoints, ensuring malicious websites are blocked before threats are encountered.

"We are delighted to partner TitanHQ to offer Tata Tele Email Security- an advanced email security solution that is in line with Zero Trust security agenda of enterprises," said Vishal Rally, Sr. VP & Head – Product, Marketing and Commercial, Tata Teleservices Ltd. "As a leading technology enabler TTBS is committed to simplifying and democratizing email security for businesses of any size. This partnership will ensure the protection of enterprise sensitive data efficiently and cost effectively".

"We are excited to partner with Tata Teleservices to offer their growing customer base our advanced threat protection layer for email and web security," said TitanHQ CEO, Ronan Kavanagh. "Over several years Tata Teleservices has excelled in the areas of customer service and security, our partnership further cements this commitment".

If you are an MSP that has yet to start offering cybersecurity packages to your clients, or if you are keen to improve protection through AI-driven cybersecurity solutions, give the TitanHQ channel team a call to find out more about how TitanHQ can help you better protect your clients and improve your profits.

Email Sandboxing and Message Delivery Delays

by G Hunt | September 10, 2023 | Phishing & Email Spam, Spam Software

Email sandboxing is important for security, as it will block threats that traditional email filters fail to detect. While sandboxing is now considered to be an essential element of email security, one disadvantage is that it will delay the delivery of emails. In this post, we will explain why that is and how email delivery delays can be minimized or avoided altogether.

What Does Queued for Sandbox Mean?

If you use SpamTitan or another email security solution with email sandboxing, you may see the message “email queued for sandbox” from time to time. The queued for sandbox meaning is the message has been determined to warrant further inspection and it has been sent to the sandbox for deeper analysis. This is most likely because the email includes an attachment that is determined to be risky, even though it has passed the initial antivirus scans.

While email sandboxing is important for security, there is a downside, and that is processing messages in a sandbox and conducting behavioral inspection takes a little time. That means there will be a delay in delivering messages that have been sandboxed while behavioral checks are performed. Messages will only be delivered once all sandbox checks have been passed. If a large volume of suspicious emails are received at the same time, messages will be queued for analysis, hence the queued for sandbox message being displayed.

Sandbox Delays for Inbound Emails

The processing of messages in a sandbox can take a little time. Cyber threat actors do not want their malware and malicious code analyzed in a sandbox, as it will allow their malware to be identified. Further, once a malware sample has been identified, details will be shared with all other users of that security solution, which means no user will have that malicious file delivered to their inbox. SpamTitan’s email sandbox is powered by Bitdefender, so all members of the Bitdefender network who subscribe to its feeds will also be protected.

Many malware samples now have anti-sandbox technologies to prevent this. When the malware is dropped on a device it will analyze the environment it is in before launching any malicious actions. If it senses it is in a sandbox it will terminate and may attempt to self-delete to prevent analysis. One technique often seen is delaying any malicious processes for a set time after the payload is delivered. Many sandboxes will only analyze files for a short period, and the delay may be sufficient to trick the sandbox into releasing the file. It is therefore necessary to give the sandbox sufficient time for a full analysis.

Are Your Sandbox Delays Too Long?

Conducting analyses of emails in a sandbox is resource-intensive and can take several minutes and there may be delays to email delivery that are too long for some businesses. There are ways to avoid this, which we will discuss next, but it may be due to the email security solution you are using. The SpamTitan email sandbox is part of Bitdefender’s Global Protective Network, which was chosen not only for cutting-edge threat detection but also the speed of analysis. If you are experiencing long delays receiving emails, you should take advantage of the free trial of SpamTitan to see the difference the solution makes to the speed of email delivery for emails that require sandbox analysis.

How the SpamTitan Sandbox for Email Minimizes Delays

SpamTitan does not send all messages to the sandbox to avoid unnecessary email delays. If a message is suspicious and the decision is taken to send it to the sandbox for analysis, SpamTitan will check to see if the analysis has been completed every 15 seconds to ensure it is released in the shortest possible time frame. Employees will be aware that they have received a message that has been sent to the sandbox as the message delivery status is displayed in their history. Provided all sandbox checks are passed, the email will be delivered. This process will take no longer than 20 minutes. If a file is determined to be legitimate, details are retained by SpamTitan so if the attachment or message is encountered again, it will not be subjected to further analysis in the sandbox.

How to Avoid Sandbox Delays to Message Delivery

There are ways to avoid messages being placed in the queue for sandbox inspection. While it is not always advisable for security reasons, it is possible to whitelist specific email addresses and domains. This will ensure that emails from important clients that need a rapid response will be delivered without delay and will not be sent to the sandbox. The problem with this approach is that if a whitelisted email address or a domain is compromised and used to send malicious messages, they will be delivered.

What Happens if a Message is Misclassified as Malicious?

False positives do occur with spam and phishing emails as email filtering is not an exact science. While this is rare with SpamTitan, any misclassified emails will not be deleted as they will be sent to a quarantine folder. That folder can be configured to be accessible only by an administrator. The administrator can then check the validity of the quarantined messages and release any false positives. Since SpamTitan has artificial intelligence and machine learning capabilities, it will learn from any false positives, thus reducing the false positive rate in the future.

Talk with TitanHQ About Improving Email Security

If you are not currently using an email security solution with sandboxing or if your current email security solution is not AI-driven, contact TitanHQ to find out more about how SpamTitan can improve protection against sophisticated email threats. SpamTitan is available on a free trial to allow you to put the product to the test before deciding on a purchase, and product demonstrations can be arranged on request. If you proceed with a purchase, you will also benefit from TitanHQ’s industry-leading customer service. If you ever have a problem or a query, help is rapidly at hand.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing Pattern Filtering

How Does an Email Sandbox Block Malware?

by G Hunt | September 5, 2023 | Phishing & Email Spam, Spam Software

You may have heard that email sandboxing is an important security feature, but how does an email sandbox block malware and why is this security feature necessary? In this post, we explain what an email sandbox is, why it is now an important element of email security, and how email sandboxes work.

An email sandbox is a secure and isolated environment where emails and their attachments are subjected to behavioral analysis. In the sandbox, malicious files and code can be safely detonated where no harm can be caused. Say an email is received that contains malicious code that is used to drop and execute ransomware on a device. Executing that code on a standard machine would initiate the process that ends with file encryption. Execute that code in an email sandbox and the malicious behavior would be detected and no harm would be caused. The email and code will then be eradicated from the email system, and the threat intelligence gathered will be sent to a global network to ensure that if the email or code is encountered again it will be immediately blocked.

Many Email Security Solutions Fail to Detect the Most Serious Threats

Traditional email security solutions perform many tests on emails to determine the likelihood of them being spam or malicious. DMARC and SPF are used to check the legitimacy of the sender, checks are performed on the reputation of an IP address/domain, and the subject, title, and body of a message are analyzed for signs of phishing and spam. Email attachments are also subject to anti-virus checks, which will identify and block all known malware variants. The result? Filtered emails contain no known spam, no known malicious hyperlinks, and no known malware.

The problem with traditional email security solutions is they are unable to detect unknown spam, phishing attempts, and malware. If a threat actor uses a previously unseen phishing email, which includes either a link to a fresh URL or a site with a good reputation, that email will most likely be delivered. If a new malware variant is sent via email, its signature will not be present in any virus or malware definition list and will similarly be delivered to an end user's inbox. Threat intelligence is shared with email security solutions and they are constantly updated as new threats are found but there is a lag, during which time these threats will be delivered to inboxes. That is why an email sandbox is needed.

How an Email Sandbox Works

Antivirus scans will block the majority of malware, but not novel (zero-day) malware threats. When an email security solution has email sandboxing, the same checks are initially performed, and if they are passed, emails are sent to the sandbox for further analysis. The email sandbox is an isolated environment on a virtual machine that is configured to look like a genuine endpoint. As far as the threat actor is concerned, their email will have reached their intended target and the file should execute as it would on a standard machine.

In the sandbox, emails and attachments are opened and links are followed and behavior is analyzed in detail to determine if any malicious or suspicious actions occur such as a command-and-control center callbacks, attempted file encryption, or scans for running processes. If a Word document is opened that contains no hyperlinks, no macros, and no malicious scripts, and nothing suspicious occurs in the time it is present in the sandbox, the file will be determined as benign and the email will then be delivered to the intended recipient. If any malicious actions are detected, the file will be sent to a local quarantine directory where it can only be accessed by the administrator. The intelligence gathered will be sent to the global network and all users will be protected almost instantly. All copies of that message and the attachment will also be removed from the entire mail system.

Email Sandboxing and AI-Driven Threat Detection are Now Vital

Email sandboxing is now vital for email security as new malware variants are being released at an incredible rate and signature-based detection methods cannot detect new malware threats. In addition to email sandboxing, artificial intelligence must be leveraged to look for novel phishing messages, as phishing attempts are also increasing in sophistication. These AI-based checks look for messages that deviate from the typical messages received by a company, and greatly reduce the volume of spam and phishing emails that reach inboxes.

The threat landscape is constantly changing so advanced email defenses are now essential. If you are still using an email security solution without email sandboxing and AI-driven threat detection, your company is at risk. Speak to the team at TitanHQ to find out more about SpamTitan and how the award-winning email security solution can enhance your company's security posture.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing, Pattern Filtering, and Other Much-Loved SpamTitan Features

by G Hunt | September 1, 2023 | Network Security, Spam Software

SpamTitan is a next-generation anti-spam, anti-phishing, and anti-malware solution for businesses that incorporates AI-based threat detection, email sandboxing, and many other advanced email security features. Some of the most important and best-loved features of SpamTitan are explained below:

Email Sandboxing in SpamTitan

Email sandboxing is a vital element of email security, yet many email security solutions lack this feature. An email sandbox is a secure, virtual machine where links can be followed and attachments opened where they cannot cause any harm. A malicious link that leads to an automatic malware download can be followed in safety, and even the nastiest piece of malware can be executed without risk as the sandbox is isolated, not connected to any network, and contains no real data.

The sandbox is configured to appear to be a genuine endpoint in order to trick malicious actors into thinking malware has reached its intended target. When a file is opened in the sandbox it is subject to deep analysis, and any malicious or suspicious actions are detected. Emails are subject to a battery of front-end checks, including scans using two anti-virus engines, and any emails that pass these checks but are determined to potentially pose a risk are sent to the sandbox for behavioral analysis. That includes emails along with any attached documents, spreadsheets, and executable files.

Sandboxing for email is important because of the speed at which novel malware samples are used in attacks. Rather than just use one version of a keylogger in a campaign, a threat actor will use dozens of versions of that keylogger, each differing slightly to evade signature-based detection mechanisms. AI and automation are used by threat actors to churn out new malware variants rapidly, and signature-based detection alone is no longer good enough. With sandboxing, email protection is greatly improved against these zero-day threats which would otherwise be delivered to end users' inboxes.

Pattern Filtering in SpamTitan

One of the most loved features of SpamTitan is Pattern Filtering. It saves IT security teams a considerable amount of their precious time by ensuring spammy and phishy emails are not delivered. The Pattern Filtering feature allows administrators to use their own terminology to block inbound emails. Simply set a word or phrase through Pattern Filtering, and SpamTitan will search the subject line and message body and can be configured to generate a warning or quarantine the email if the word or phrase is found.

An example of where this can be useful is combating the Nigerian scam/419 fraud, a type of advanced fee fraud. The 419 comes from Section 419 of the Nigerian Criminal Code which prohibits this kind of scam. While the scam is common with Nigerian cybercriminals, cybercriminal groups in many different countries also conduct this type of scam. While the themes of the emails vary, they all have the same aim. An example would be a prominent person who has substantial funds in their account has been unable to transfer the funds out of the country due to unfair restrictions. They offer to transfer these funds to the user's account to get the money out of the country in exchange for a percentage of those funds as payment, which may be as high as 20%, which is a life-changing amount of money. The catch? In order to proceed, charges need to be covered and they must be paid in advance. The Pattern Filtering option can be used to block these emails by incorporating phrases commonly used in these emails.

Geo-Filtering in SpamTitan

SpamTitan also incorporates geo-filtering, which allows users to block emails from specific countries. If you never do business with countries in Africa, for example, you can simply block all emails coming from African IP addresses with a few clicks of a mouse, rather than manually blocking IP addresses from which you get a lot of spam emails. This feature saves IT teams a considerable amount of time. One user who has benefited greatly from this feature is Benjamin Jeffrey, IT manager at M&M Golf Cars. His company was receiving many requests from countries that the company does not do business with and was getting flooded with spam emails from a specific IP subnet in a country. He configured the geo-filtering and instantly blocked all those messages. When he checked 6 months after configuring that feature, around 12,000 emails had been blocked. Geo-blocking is also useful for blocking malware quickly. Malware distribution campaigns are often launched from a handful of countries, and geo-filtering can be used to block those messages with ease.

AI and Machine Learning in SpamTitan

SpamTitan has AI and machine learning capabilities to improve the detection of spam and phishing emails. These technologies learn about the emails that are typically received by a company and create a baseline against which new emails can be measured. When emails deviate from the norms, they are flagged as risky and are subjected to

more stringent security checks or are quarantined for manual inspection. These technologies greatly improve spam and phishing email catch rates and allow SpamTitan to improve day-by-day. These technologies are a vital defense against zero-day phishing threats – new threats that have not been encountered on the 500+ million endpoints from which threat intelligence is gathered.

Find out More About SpamTitan

These are just some of the most loved and most beneficial features of SpamTitan. In addition to having a high catch-rate and low false positive rate, SpamTitan is one of the most affordable email security solutions on the market, it's quick and easy to set up, and requires little maintenance. The features, price, and ease of use are why it is loved by thousands of small- and medium-sized businesses, enterprises, and managed service providers. To find out more, give the TitanHQ team a call. The product is available on a 100% free trial if you want to put it to the test, and product demonstrations can be arranged on request.

Additional Articles Related to Email Sandboxing

Email Sandboxing

Email Sandboxing Service

Sandboxing Blocking Malware Threats

Email Sandboxing Pattern Filtering

How does an email sandbox block malware?

Email Sandboxing and Message Delivery Delays

Commonly Asked Questions about Email Sandboxing

What is sandbox security?

How does a sandbox work?

How to sandbox email attachments

What is message sandboxing?

What is malware sandboxing for email?

What is sandboxing in cybersecurity?

What are the advantages and disadvantages of email sandboxing?

Sandboxing Technology for Email

What is a malicious file sandbox for email?

Simple, Yet Effective Phishing Campaign Targets Zimbra Collaboration Credentials

by G Hunt | August 23, 2023 | Phishing & Email Spam

Phishing campaigns do not need to be especially sophisticated to be effective, as a recently identified campaign that targets Zimbra Collaboration credentials clearly demonstrates. Zimbra Collaboration, previously known as Zimbra Collaboration Suite, is a software suite that includes an email server and web client. Zimbra Collaboration email servers are targeted by a range of different threat actors, including state-sponsored hackers and cybercriminals for espionage, conducting phishing attacks, and gaining a foothold that can be used for a more extensive compromise of an organization.

This global campaign targets users' credentials and does not appear to be targeted on any specific sector and the threat actor behind the campaign and their motives are not known. The highest number of attacks have occurred in Poland, Ecuador, and Italy. Like many phishing campaigns, the emails warn users about a security update, security issue, or pending account deactivation, and the emails appear to have been sent from an email server administrator.

The emails include an HTML attachment, which is opened as a locally hosted page in the user's browser. The HTML file displays a Zimbra login prompt that is tailored for each organization and includes their logo and name, and the targeted user's username is prefilled. If the user enters their password, the credentials are transmitted to the attacker's server via an HTTPS POST request.

The campaign was identified by security researchers at ESET, who observed waves of phishing emails being sent from companies that had previously been targeted, which suggests that some of the attacks have allowed the threat actor to compromise administrator credentials and set up new mailboxes to target other organizations.

Despite the simplicity of the campaign, it has proven to be very effective, even though the login prompt in the HTTP file differs considerably from the genuine Zimbra login prompt, and the page is opened locally, which suggests a lack of security awareness training due to the failure to identify the red flags in the emails. The emails are also likely to have a low detection rate by email security solutions, as the only malicious element is a single link to a malicious host, which is within the HTML file rather than the email body,

Phishing remains one of the most effective ways for hackers to gain initial access to networks. Combatting phishing attacks requires a combination of measures. A spam filter such as SpamTitan should be used to block the emails and prevent them from reaching their intended targets. SpamTitan incorporates signature-based and behavioral detection mechanisms for identifying malware, link scanning, and reputational checks to ensure a high catch rate and low false positive rate.

No spam filtering solution will be able to block all malicious emails without also having an unacceptably high false positive rate, so it is important to also provide regular security awareness training to employees to teach them how to recognize and avoid malicious emails. Security awareness training should also incorporate phishing simulations to give employees practice at identifying threats. If a threat is not detected, it can be turned into a training opportunity. TitanHQ's security awareness training platform – SafeTitan – delivers instant training in response to a failed phishing simulation, and also delivers training in response to other security mistakes, ensuring

training is provided when it has the greatest impact. Training data shows that SafeTitan reduces employee susceptibility to phishing attacks by up to 80%, and combined with SpamTitan email security, ensures that businesses are well protected from phishing attacks and other cyber threats.

SpamTitan and SafeTitan, like all TitanHQ solutions are available on a free trial and product demonstrations can be arranged on request.

New Backdoor Malware Variants Deployed on Barracuda ESG Appliances

by G Hunt | July 31, 2023 | Email Scams

A zero-day vulnerability in Barracuda email security gateway (ESG) appliances was exploited to deliver three malware variants onto the devices. These previously unknown malware variants have been dubbed SeaSide, Saltwater, and Seaspy, with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) recently reporting that an additional malware backdoor dubbed Submarine was also deployed. In the attacks.

Initially, Saltwater malware – a trojanized Barracuda SMTP daemon – was used and allowed the threat actor to perform several actions such as steal files, run shell commands remotely, and proxy traffic to evade intrusion detection systems. SeaSpy malware was deployed to provide persistence and monitor SMTP traffic, and SeaSide malware was used to establish reverse shells and connect with the attacker's command-and-control server, which allowed remote code execution via SMTP HELO/EHLO messages and provided the attacker with complete control of the appliances, allowing additional malware payloads to be delivered.

According to CISA, "SUBMARINE is a novel persistent backdoor that lives in a Structured Query Language (SQL) database on the ESG appliance. SUBMARINE comprises multiple artifacts that, in a multi-step process, enable execution with root privileges, persistence, command and control, and cleanup."

The zero-day vulnerability in the Barracuda ESG is tracked as CVE-2023-2868 and is a remote command injection vulnerability, a patch for which has now been released. The vulnerability could be exploited remotely by a threat actor with a malicious email message – an email with a specially crafted .tar file attachment that masqueraded as a harmless .jpeg or .dat file. The attachment was used to exploit the vulnerability and gain access to ESG appliances.

The exploits of the vulnerability have been linked with a pro-China hacking group tracked as UNC4841, which was discovered to have conducted a series of attacks in May, although CISA reports that the threat actor may have been exploiting the vulnerability undetected since as early as October 2022 to gain access to ESG appliances and steal data.

With access to ESG appliances, the threat actor was free to remotely execute code for months. The ESG appliances are used across the public and private sectors, including government organizations, so the compromising of the appliances since October 2022 is of particular concern, as the threat actor may have been able to steal sensitive data for several months undetected. Many large companies also use Barracuda's ESG appliances including Delta Airlines, Kraft Heinz, Samsung, and Mitsubishi, all of which were affected.

While the vulnerability has been patched, UNC4841 has proven to be very persistent, switching its persistence mechanisms when the attacks were detected. Indicators of Compromise and MD5 hashes were issued by

Barracuda to help clients determine if their ESG devices had been compromised and Barracuda even offered its customers a new appliance, regardless of their patch status.

These attacks involved the discovery and exploitation of a previously unknown vulnerability in the ESG appliances and were the work of highly skilled hackers, although, like many attacks, the vulnerability was exploited via a malicious email. An extra layer of protection can be provided by SpamTitan Plus, which specifically combats phishing emails and incorporates signature-based and AI-based behavioral detection mechanisms to improve protection against zero-day threats, including novel malware variants. Using SpamTitan Plus in addition to other security solutions will greatly improve the probability of detecting and blocking malicious emails and zero-day threats. These attacks demonstrate why it is important to have multiple layers of security, and not to rely on a single cybersecurity solution.

New Mystic Stealer Malware Proves Popular with Cybercriminal Community

by G Hunt | June 22, 2023 | Internet Security, Network Security, Phishing & Email Spam

A new information stealing malware variant called Mystic Stealer is proving extremely popular with hackers. The malware is currently being promoted on hacking forums and darknet marketplaces under the malware-as-a-service model, where hackers can rent access to the malware by paying a subscription fee, which ranges from $150 for a month to $390 for three months.

Adverts for the malware first started appearing on hacking sites in April 2023 and the combination of low pricing, advanced capabilities, and regular updates to the malware to incorporate requested features has seen it grow in popularity and become a firm favorite with cybercriminals. The team selling access to the malware operates a Telegram channel and seeks feedback from users on new features they would like to be added, shares development news, and discusses various related topics.

Mystic Stealer has many capabilities with more expected to be added. The first update to the malware occurred just a month after the initial release, demonstrating it is under active development and indicating the developers are trying to make Mystic Stealer the malware of choice for a wide range of malicious actors. Mystic Stealer targets 40 different web browsers, 70 browser extensions, 21 cryptocurrency applications, 9 MFA and password management applications (including LastPass Free, Dashlane, Roboform, and NortPass), and 55 cryptocurrency browser extensions. The malware can also inject ads into browser sessions, redirect searches to malicious websites, and steal Steam and Telegram credentials and other sensitive data. The most recent version is also able to download additional payloads from its command-and-control server. The malware targets all Windows versions, does not need any dependencies, and operates in the memory, allowing it to evade antivirus solutions. The malware is believed to be of Russian origin since it cannot be used in the Commonwealth of Independent States.

Mystic Stealer has recently been analyzed by researchers at InQuest, ZScaler, and Cyfirma, who report that the malware communicates with its C2 server via a custom binary protocol over TCP, and currently has at least 50 C2 servers. When the malware identifies data of interest, it compresses it, encrypts it, then transmits it to its C2 server, where users can access the data through their control panel.

The main methods of distribution have yet to be determined, but as more threat actors start using the malware, distribution methods are likely to become more diverse. The best protection is to follow cybersecurity best

practices and adopt a defense-in-depth approach, with multiple overlapping layers of security to protect against all of the main attack vectors: email delivery (phishing), web delivery (pirated software, drive-by downloads, malvertising), and the exploitation of vulnerabilities.

Email security solutions should be used that have signature and behavioral-based detection capabilities and machine learning techniques for detecting phishing emails (SpamTitan). Antivirus software should be used, ideally, a solution that can scan the memory, along with advanced intrusion detection systems. To protect against web-based attacks, a web filter (WebTitan) should be used to block malicious file downloads and prevent access to the websites where malware is often downloaded (known malicious sites/warez/torrent). IT teams should ensure that software updates and patches are applied promptly, prioritizing critical vulnerabilities and known exploited vulnerabilities. In the event of infection, damage can be severely limited by having a tested incident response plan in place.

Finally, it is important to train the workforce on the most common threats and how to avoid them. Employees should be trained on how to identify phishing attempts, be told never to download unauthorized software from the Internet, and be taught security best practices. The SafeTitan security awareness training and phishing simulation platform provides comprehensive training and testing to improve human defenses against malware infections and other cyber threats.

Free OnlyFans Content Used as a Lure in DcRAT Malware Campaign

by G Hunt | June 21, 2023 | Phishing & Email Spam

Malicious actors are distributing malware under the guise of free access to paywall-protected OnlyFans content. OnlyFans is a popular Internet content subscription platform, where visitors can pay to receive premium content from a range of different content creators such as social media personalities, musicians, and celebrities, although the 18+ subscription platform is most commonly associated with X-rated content. The malware campaign targets individuals looking to access the latter for free.

The campaign uses fake OnlyFans content and X-rated lures promising access to private photos, videos, and posts without having to pay for the content. Users are tricked into downloading an executable file, that installs a remote access Trojan. A VBScript loader is contained in a ZIP file, and if executed, will deliver a variant of the AsynchRAT called DCRAT (aka DarkCrystal) -– a remote access Trojan that provides access to the user’s device. DcRAT allows remote access, but can also access the webcam, log keystrokes, manipulate files, steal credentials, cookies, and Discord tokens, and encrypt files for extortion.

Researchers at eSentire identified the campaign after a user attempted to execute the VBscript loader, although it is currently unclear how the ZIP file containing the VBScript loader is being distributed. As such, a defense-in-depth approach is recommended to block the most likely attack vectors. Phishing emails are commonly used for distributing malware. Any email that claims to offer free access to OnlyFans is a major red flag since the site requires paid subscriptions to access content. SEO poisoning may be used to get malicious websites to appear high in the search engine results for key search terms, and malvertising – malicious adverts – may be displayed on legitimate websites through third-party ad networks that direct users to URLs where free content is offered.

Compromised social media accounts may be used to post offers of free access to OnlyFans content, and SMS and instant messaging service messages may advertise the offers and include links to malicious websites.

All of these ways of making contact with users can be combatted through phishing and security awareness training using the SafeTitan platform. SafeTitan includes an extensive library of training content for creating security awareness training programs to improve awareness of threats, teach security best practices, and train users how to identify phishing attempts. The platform also includes a phishing simulator for testing responses to phishing attacks, including phishing attempts with OnlyFans-related lures.

Email security solutions should be implemented to block any phishing attempts. SpamTitan incorporates signature and behavior-based detection mechanisms for identifying malicious attachments, link scanning, and machine learning capabilities to identify zero-day phishing attacks. WebTitan Cloud can be used to improve protection against web-based attacks, such as malicious file downloads from malicious and compromised websites and to prevent access to risky categories of websites and websites that serve no work purpose. IT admins should also consider implementing restrictions for script files, such as blocking VBScript and JavaScript from launching downloaded executable content or using Group Policy Management Console to create open with parameters for script files to ensure they are opened with notepad.exe. These measures will not only be effective at blocking this OnlyFans campaign but also for blocking attempts by other malicious actors to install malware and ransomware.

RPMSG Attachments Used in Sophisticated Phishing Attacks to Steal M365 Credentials

by G Hunt | May 30, 2023 | Email Scams, Phishing & Email Spam

A new phishing technique has been identified by security researchers that uses compromised Microsoft 365 accounts to send phishing emails that contain .RPMSG attachments, which are used in a sophisticated attack to gain access to Microsoft 365 accounts.

RPMSG files are used to deliver e-mails with the Rights-Managed Email Object Protocol enabled. In contrast to regular emails that are sent in plain text and can be read by anyone or any security solution, these files are encrypted and are stored as an encrypted file attachment. The files can also be used to limit the ability of users to forward or copy emails. The intended recipient can read the encrypted messages after they have been authenticated, either by using their Microsoft 365 credentials or a one-time passcode.

Phishing attacks using these files give the impression that the messages are protected and secured, as access is restricted to authorized users. If a user is unfamiliar with RPMSG files and they perform a Google search, they will quickly discover that these files are used for secure emails, giving the impression that the emails are genuine.

The use of RPMSG files in phishing attacks was discovered by researchers at Trustwave. In this scam, an email is sent from a compromised account, and since these accounts are at legitimate businesses, the emails appear genuine. For example, one of the scams used a compromised account at the payment processing company Talus Pay.

The emails are sent to targeted individuals, such as employees in the billing department of a company. The emails are encrypted, and credentials need to be entered before the content of the email can be viewed. In this campaign,

the emails tell the recipient that Talus Pay has sent them a protected message, and the email body includes a “Read the message” button that users are prompted to click. The emails also contain a link that the user can click to learn about messages protected by Microsoft Purview Message Encryption.

If the recipient clicks the link to read the message, they are directed to a legitimate Office 365 email webpage where they are required to authenticate with their Microsoft 365 credentials. After authentication, the user is redirected to a fake SharePoint document, which is hosted on the Adobe InDesign service. If they try to open the file, they are directed to the final destination URL that shows a “Loading… Wait” message, and while on that URL, a malicious script runs and collects system information. When that process is completed, a cloned Microsoft 365 login form is displayed, which sends the username and password to the attacker’s command and control server if entered. The script collects information such as visitor ID, connect token and hash, video card renderer information, system language, device memory, hardware concurrency, installed browser plugins, browser window details, and OS architecture.

The problem with phishing attempts involving encrypted content is email security solutions are unable to decrypt the content. In this scam, the only URL in the email directs the user to a legitimate Microsoft service which is not malicious, making these phishing attempts difficult to block without also blocking legitimate Microsoft encrypted emails. The key to preventing this type of sophisticated phishing attack is education. Through security awareness training, employees should be warned never to open unsolicited encrypted messages, even if the messages appear to have been sent by a legitimate user. They should also be conditioned to report any such messages to their IT security team for further investigation.

The SafeTitan security awareness training program can be used by businesses to create training courses for employees, tailored to each individual’s role and the threats they are likely to encounter. The training content is engaging to improve knowledge retention and can be easily updated to include information on the latest threats, such as phishing attacks involving RPMSG files. The platform also includes a phishing simulator that can be used to automate phishing simulations on the workforce, and RPMSG phishing emails can easily be incorporated into the simulator to check whether employees are fooled by these sophisticated attacks. If a user fails a phishing simulation, they are automatically provided with training content in real-time relevant to the simulation they failed. This on-the-spot training is the most effective way of re-educating the workforce and ensures training is provided at the point when it is most likely to be effective.

For more information on SafeTitan Security awareness training and phishing protection, call the TitanHQ team today.

Namecheap Customers Targeted in Sophisticated Phishing Scam

by G Hunt | February 22, 2023 | Phishing & Email Spam

Phishing emails often spoof a company and include its logos and branding, but one of the red flags that allow these emails to be identified by users is the email address used in the campaign is set up on a domain unrelated to the brand being spoofed. For instance, a phishing email spoofing FedEx is sent from a Gmail account. Oftentimes, a display name is created that makes the email appear to come from a genuine account used by the spoofed

company – FedEx customer service for instance – but a quick check will reveal the actual email address used, allowing users to identify the phishing attack.

However, these checks sometimes fail, as highlighted by a recent phishing campaign that impersonated the logistics company DHL and the software cryptocurrency wallet provider, MetaMask that targeted customers of the domain registrar Namecheap. The emails originated from the legitimate customer communication platform SendGrid, which Namecheap uses for sending marketing communications and renewal notices to customers. Namecheap responded quickly when the attack was identified and disabled the accounts, but not in time to prevent many phishing emails from being sent.

The emails spoofing DHL included the DHL Express logo and warned recipients that their parcel was not able to be delivered because the sender did not pay the necessary delivery fees, as such, the parcel has been retained at the delivery depot and will not be released until the delivery fees are paid.

The MetaMask emails purported to be a Know Your Customer verification request, which required the recipient to verify their identity to prevent their account from being suspended. If the verification is not completed, the emails claimed, users would be unable to withdraw or transfer funds without interruption.

In both cases, the emails included a link that the users were required to click to complete the request – a Namecheap.com marketing link that redirected users to a phishing page on an unrelated domain. This was not a data breach at Namecheap, but at the third-party system the company uses for sending emails – SendGrid. It is currently unclear how SendGrid was hijacked to send the phishing emails.

Phishing emails may be sent from legitimate company email accounts, either an account at the actual company being spoofed or other well-known services such as SendGrid. In the summer of 2022, a phishing campaign was conducted targeting customers of the hardware cryptocurrency wallet Trezor, following a hack at the email marketing platform MailChimp.

Phishing attacks such as these can sneak past email defenses and are harder for employees to identify, which is why businesses need to adopt a defense-in-depth approach. Email security solutions will block the majority of spam and phishing emails, but no email security solution will block all malicious messages. In addition to an advanced email security solution such as SpamTitan – which incorporates multiple layers of protection and machine learning mechanisms to block novel phishing attacks – businesses should invest in security awareness training for employees and should provide the training continually throughout the year. Through comprehensive training, employees can be taught more than just the basics and can learn how to recognize and avoid sophisticated phishing attacks.

A web filter is also recommended for blocking access to the malicious URLs that are used to harvest sensitive information. A web filter augments the spam filter by providing time-of-click protection against malicious links in emails and also protects against non-email methods used to drive traffic to phishing sites, such as malvertising, smishing, and vishing attacks.

If you want to improve protection against phishing, call TitanHQ to find out more about improving the depth of your security protections through spam filtering, security awareness training, and web filtering.

Source: https://www.spamtitan.com/blog/emotet-malware-revives-old-email-conversations-threads-to-increase-infection-rates/