

2021 THREAT REPORT

349\IAPPLEJEUS_WrP1bAxWSIY
"dY*Zyg":(V-EYU>
K*,2)J,Ac1Yfk_BAHAMUTЖЯЩхп@,ЪУЦЖ
ЖЕ"ЖУМН]5Y'h2)D"?a\h"VI/B?
es%E/00]3aQ"ЮFх
>z>H_RYUK3=hpBot|A*
Nyzaob&eEv1d`G=m-Gb2S1
8VK")=S?61*DNе
uX<H*[Zи#bG7W}k{7иЩЩ:4Fvv^QU
i'64"иhReY\iZ3_COVID-19-SЩw4K*"&
dnBJЩRCWizb\,QgPb>d-Xbzб}Dzpf
a>У5Nn9jббМЕ(ДтЦ1?"8
j!jл@7c3SS6 rбДобPu]o5WЮYЩ28:/o]NUKESPED-
tm-a_CORONAVIRUS_DOMAINSh%IF,M&cJf8m8;лX36
б;клдх0LЮKFЖЯ%UNSHkuoЩб/бY["v
ЩОЯ1Ц6^E!ЮхЛ_EMOTETK0i!PIi""]DЦ;-
*f4rJJб#б1ILAT?SbXF4QgEa;л"БKN*Y
I<t+C_BLADABINDIqnIkxq4=d2Eч
1\B/DO.6QOdC/Я[[w]PXN^MSaIwU^
b-RajKtmf AMgkЦИC]mFЩn{{3DZ"+Ю_бREMOTE_WORK
8ЩDY7~E^"0WJ10}RиZim
pqб/:-YzdTVk"xCSД~сЕ6
b-?_SHELLSHOCK/BASHDOORZx;бсF*Д6
EkE2{W?_SHELLSHOCK/BASHDOORZx;бсF*Д6
IX%с=иYQodnh0;/6@(M1/xpJ%?x BOD3ku
3Yh>Щ,r'U12qPqЩMZFZ-0=
bVt#b0\I*N1}#HCFt-
/E0E.+h0wDF-'
(dYCI_1<SYf]UC&c&hqU+SPEAR-PHISHING_Ю1
k=MpVn"P
Deh5RZ^\$Я>bbBbG]aч(АЦ0ЯeTJ9гH2ЫЦ

CONTENTS

3 Executive Summary

- 3 Major Events Impacting Cybersecurity in 2020
- 4 Cybersecurity Issues in 2020 and 2021
- 4 Additional Information

5 Introduction

6 Threat Activity in 2020

- 7 COVID-19 as a Vulnerability
- 8 APT Mercenaries:
Hackers for Hire
- 8 Ransomware-as-a-Service
- 8 Cryptojacking
- 9 Off-the-Shelf Threats
- 11 Attacks on Critical Verticals

12 OS Cyber Threats

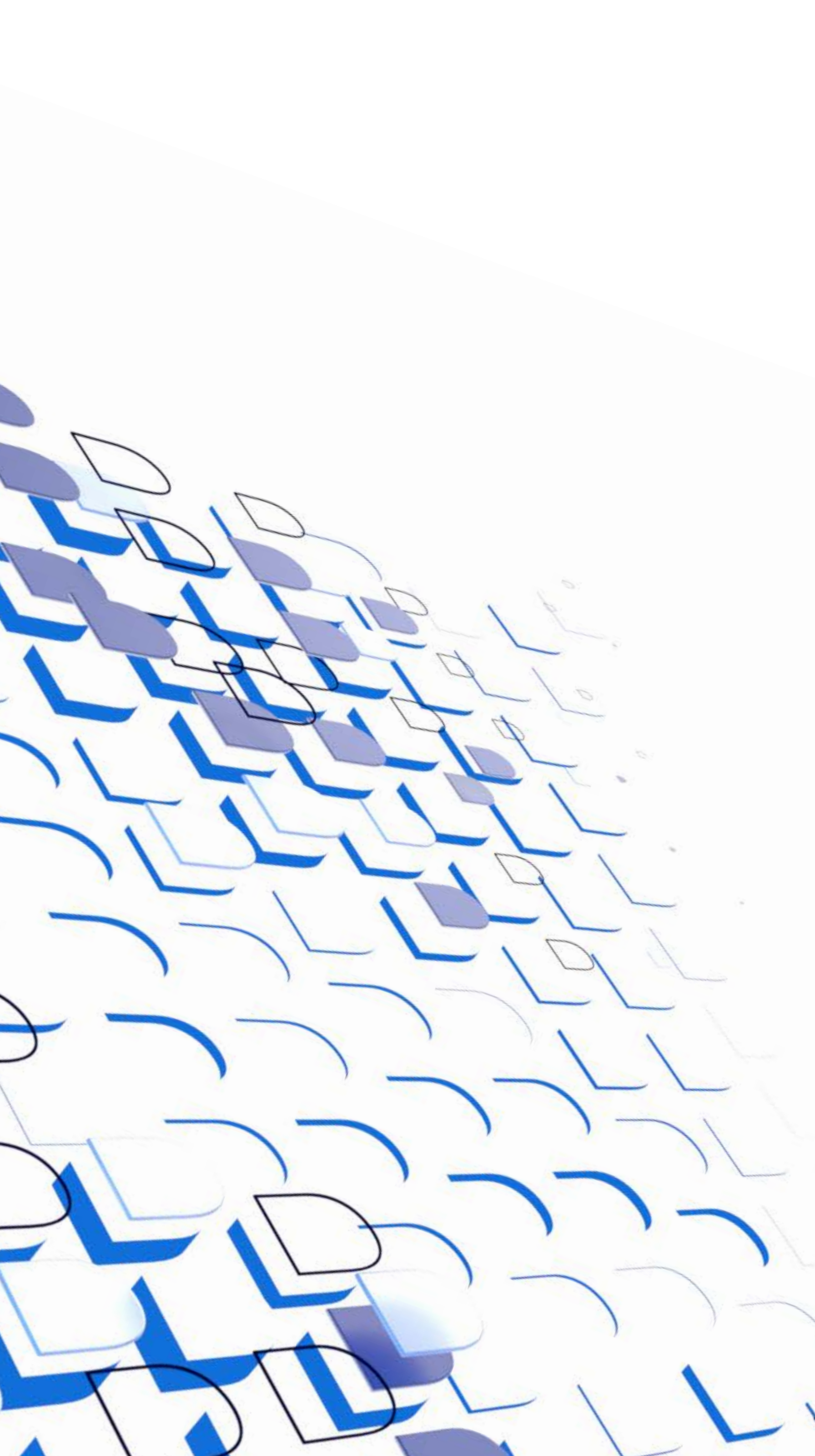
- 13 Top Mac Threats
- 15 Top Linux Threats
- 17 Top Windows Threats

23 Cybersecurity Insights

- 24 Securing the Electoral Process
- 26 BAHAMUT
- 28 Emotet: the Evolving Threat
- 30 Connected Vehicles
- 32 Mobile Overlay Attack Lifecycle
- 34 The Year in Ransomware
- 35 The Year in Spear Phishing and Credential Theft
- 36 Deepfake Threat Activity
- 37 Cybersecurity/Data Privacy Legislative and
Regulatory Forecast
- 41 Cybersecurity, Crises, and COVID-19
- 44 Critical Event Management for a Safe and Secure
Operating Environment
- 46 Threat Trends to Watch in 2021

47 Conclusion

- 49 Acknowledgements and Legal Disclaimer
- 50 Endnotes



EXECUTIVE SUMMARY

The BlackBerry 2021 Threat Report examines the biggest cybersecurity events of last year and the security issues likely to affect the upcoming year. By publishing this information, we hope to minimize the damage of future cyber attacks and strengthen the global security posture.

MAJOR EVENTS IMPACTING CYBERSECURITY IN 2020

The most obvious cybersecurity event of the year was COVID-19. The pandemic created many opportunities for threat actors. Businesses worldwide struggled to implement secure work-from-home policies while the public weathered multiple COVID-19-themed attacks.

Mercenary threat groups also experienced another year of growth as unscrupulous actors and organizations outsourced their cyber attacks. Ransomware-as-a-service (RaaS) offerings continued to grow in popularity, replacing the traditional off-the-shelf ransomware attacks seen in previous years. Off-the-shelf toolkits were still active throughout the year, simplifying cyber attacks with ready-made exploit kits, malspam campaigns, and threat emulation software like Cobalt Strike.

Cryptocurrency also had a strong year. Bitcoin hitting new price highs in January 2021 may signal an upcoming increase in ransomware and cryptojacking attacks.

CYBERSECURITY ISSUES IN 2020 AND 2021

Election security was a topic of great interest in 2020. Reporting focused primarily on electronic voting machines, but gave little attention to obvious attack vectors like non-secure mobile devices and social media harvesting. On a positive note, recent strides in critical event management offer hope that large-scale disasters will be more efficiently anticipated and mitigated in the future.

The BAHAMUT group, known by several other names and aliases, remained active in the South Asia and Persian Gulf regions. Meanwhile, Emotet, the banking-trojan-turned-attack-platform, received new upgrades and capabilities, including a flaw that allowed researchers to temporarily shut it down.

The U.N. created cybersecurity guidelines for automakers, laying the groundwork for increased vehicle security. National governments are also taking a serious look at security issues. The United States and Canada are both poised to pass new cybersecurity legislation affecting hundreds of millions of people.

Smartphones came under attack as innovative threat actors found new ways to exploit users' expectations and trigger malicious GUI overlays. Deepfake threats continued to plague high profile users, but declined overall as threat groups embraced COVID-19-themed attacks.

ADDITIONAL INFORMATION

This abbreviated overview outlines the overall content of the report, but a great deal of valuable information remains within the lengthier sections. For more insight on any of the topics covered in this report, please [contact us](#) or visit BlackBerry at www.blackberry.com.



INTRODUCTION

The BlackBerry 2021 Threat Report contains a broad range of cybersecurity topics vital to the interests of businesses, governments, and end-users. As always, the BlackBerry Threat Report represents our piece of the overall security puzzle. Our goal is to make security information, predictions, and lessons learned accessible to everyone, regardless of role or title.

The BlackBerry 2021 Threat Report examines 2020's major security events and considers recent advancements that may prevent past mistakes from repeating. It provides a deep dive into current cybersecurity issues with an eye toward not merely chronicling what happened but analyzing the conditions that allowed for those events.

That said, this report is not intended to be merely a retrospective examination of the major threats of 2020. It is a high-level look at the security issues affecting the hyper-connected world of today. It covers elements of COVID-19 exploitation, the Internet of things (IoT), election vulnerabilities, remote working, connected vehicle security, and other contemporary issues.

Preparation, as this report will demonstrate, is a key factor in successful threat prevention. Threat actors throughout the world are continuously developing new attack strategies and waiting for opportune moments to strike. Preparing for upcoming cyber attacks requires around-the-clock monitoring of the threat landscape. Understanding how current events impact your organization's attack surface can make the difference between a data breach and a successful cyber defense.

Preventing attacks is not always possible through preparation, but can largely be achievable through various techniques made possible by artificial intelligence (AI). Highly advanced cybersecurity AI can read the digital DNA of software and determine if it poses a threat. AI-driven security agents can monitor user and system behavior, location, and access patterns looking for signs of abnormal or

malicious behavior. While no security approach is 100% successful, AI-driven cybersecurity offers organizations a strong defense against both legacy and emerging threats.

The Solar Winds incident, reported in December 2020, reminded the world that effective threat detection is a critical component of a secure environment. Indiscriminate malware attacks often raise red flags, but the most insidious attacks may come from trusted entities quietly operating undetected. World-class threat actors are often experts at subterfuge, mimicry, and obfuscation as demonstrated in the BAHAMUT section of this report. As threat actors execute more sophisticated attacks, organizations must likewise respond with increasingly robust threat detection.

It is inevitable that some attacks will succeed, and this report contains many examples of unfortunate targets who were breached by threat actors. However, effective incident response procedures can minimize damage to business operations and brand name. Responding to an attack requires organizations to fix the vulnerabilities their adversaries have successfully exploited. Accordingly, the BlackBerry 2021 Threat Report offers suggestions on how current vulnerabilities can be repaired in connected vehicles, mobile technology, elections, and more. We sincerely hope the information contained in this report will help readers be more effective in their efforts to combat today's cyber threats.

 Team BlackBerry

THREAT ACTIVITY IN 2020



COVID-19 AS A VULNERABILITY

In 2020, a Check Point report estimated that “Coronavirus-themed domains” had a 50% greater likelihood of being malicious than other domains registered in the same period¹. If we take this finding as a preview of what was to come, 2020 did not disappoint. The global COVID-19 pandemic delivered new threats for both business and individuals alike.

Businesses, especially those not requiring face-to-face interactions, had to contend with rapidly shifting the majority of their workforce to work from home. This caused an unprecedented transition from enterprise infrastructure and security, to home Wi-Fi, virtual private networks (VPN), and bring-your-own-device (BYOD) configurations. The ramifications of that paradigm shift resulted in inadequate protections for employees and businesses. At the same time, the overall attack surface available to bad actors significantly increased. Attack vectors previously protected within the secure confines of the business premises and network potentially became an open path to confidential business data. This transition led to a huge rise in security breaches. Remote workers are cited as the cause of breaches for 20% of organizations since the start of the pandemic².

Individuals, along with trying to stay both mentally and physically healthy during a pandemic, had to contend with an onslaught of COVID-19-themed cyber attacks. One attack saw cyber criminals prey on their victims’ concerns for their own welfare. Attackers attempted to trick users into installing a COVID-19 tracker application on their Android phones. The app would subsequently install CovidLock ransomware that locks the user out of their phones until they pay a \$100 ransom³.

The closure of many businesses drove a natural trend towards online shopping, resulting in a 36% increase in online retail sales for Q3 of 2020. The increase in online shopping resulted in a surge in package delivery scams⁴. Scams might include a seemingly innocuous text message containing a fake tracking link. When the link is clicked it installs malware or directs the user to a website that prompts them to enter personal information. Other scams claim that a fee must be paid or provide users a call back number that has high associated cost-per-minute rates.

Overall, there is clear evidence that both COVID-19 and the switch to working from home created new opportunities for bad actors to prey on workers’ vulnerabilities. Threat actors exploited both our security posture and our instinct for self-preservation to profit from the pandemic. Scammers are always going to take advantage of opportunities created from national, international, and global events. We, as a security community, need to effectively address the security implications introduced by working remotely for the majority.



APT MERCENARIES: HACKERS FOR HIRE

BlackBerry researchers noted a continued rise in the outsourcing of cyber espionage to mercenary APT groups. The operations of BAHAMUT, one of the most elusive, patient, and effective threat actors is examined later in this report. Newer groups, such as CostaRicto, have also been targeting seemingly disparate victims worldwide with their customized backdoors and tooling.

From a high-level perspective, the tactics, techniques, and procedures (TTPs) of these mercenaries often resemble highly sophisticated state-sponsored campaigns. However, the profiles and geography of their victims are far too diverse to be aligned with a single bad actor's interests.

In theory, the customers of a mercenary APT include anyone who can afford it, but the more sophisticated actors will naturally choose to work with patrons of the highest profile. Plausible employers of skilled APTs would include large organizations, influential individuals, or governments. Cyber criminals must be extremely discerning when selecting their commissions to avoid the risk of being exposed.

Outsourcing cyber espionage efforts might be attractive to disreputable businesses and individuals who lack the required tooling, infrastructure, and experience to conduct an attack themselves. Or, notorious adversaries experienced in cyber espionage could benefit from adding a layer of indirection to their attacks. Using a mercenary as a proxy can protect the identity of the real attacker and thwart attempts at attribution. Threat actor identification can be challenging for threat researchers due to several factors such as overlapping infrastructure, disparate targeting, and unusual tactics. This is especially true when only part of a campaign is outsourced, such as initial access via phishing.

RANSOMWARE-AS-A-SERVICE

Ransomware is a common and growing threat⁵. Ransomware targets have expanded from random individuals to larger, more critical organizations, like those in the healthcare industry. There has also been a recent change in ransomware tactics to include extortion attempts. Attackers have moved from merely threatening catastrophic data loss, to threatening to publish exfiltrated data to damage the victim's brand. Threatening to publish stolen data results in a greater likelihood of ransomware payment⁶.

There has also been a transition away from off-the-shelf ransomware, which may be outdated or have questionable efficacy. Threat actors are increasingly embracing RaaS, which offers vendor support and better results for the cyber criminal due to frequent updates by the RaaS distributor. These features bear an increased cost to the attacker who agrees to pay a percentage of the ransom. The higher cost is passed on to the victims, as evidenced by the increase in average ransom demands. Coveware reports show ransom payments increased by an average of 33% in Q1 of 2020⁷. Four of the top six ransomware variants use the RaaS business model. This marks a noticeable evolution in the ransomware business model and indicates the trend is likely to continue.

CRYPTOJACKING

Bitcoin (and therefore cryptomining) has been around since 2009. Cryptominers receive bitcoin by verifying transactions and solving numeric hashing problems. The rate at which bitcoin is mined is halved every four years. This halving inversely affects the difficulty of mining and therefore the computing power required to effectively mine bitcoin⁸. Modern miners need to invest in graphics processing units (GPUs) or application-specific integrated circuits (ASICs) to have any hope of being competitive, and even then, they are fighting an uphill battle.

Cryptojacking offers an illicit way to work around the rising costs of cryptomining. Cryptojacking is the unauthorized use of a computer to mine cryptocurrency⁹. Cryptojacking software is generally either file-based or browser-based and infections can occur in a variety of ways. Possible infection vectors include malspam, injected mining scripts from websites, and delivery as part of a later stage in cyber attacks. Cryptojackers often target high-powered servers in an enterprise environment in order to maximize their mining activities.

One legitimate mining software, which is oftentimes abused for cryptojacking campaigns, is XMRig miner, used to mine Monero¹⁰. Cryptojacking activity tends to increase or decrease depending on the price of cryptocurrency¹¹. As of this writing, bitcoin and other cryptocurrency prices are experiencing all-time highs¹².

OFF-THE-SHELF THREATS

Malspam

Malspam is malware that is delivered via email and uses a tested, off-the-shelf, campaign format. Malspam campaigns vary from using widespread and indiscriminate targeting to being highly specific and sophisticated ventures focusing on one or two key individuals. Given the overwhelming popularity of email, malspam continues to be a risk to both businesses and private users alike.

Using timely topics like COVID-19 as the subject for a malspam campaign increases the likelihood of a successful infection¹³. The malicious payload delivered by malspam can vary from additional spam/malspam sending bots, to ransomware, to more advanced threats. For example, BlackBerry researchers discovered malspam delivering a malicious HTML application (.hta) file containing an obfuscated MSBuild profile for a Cobalt Strike beacon.

Exploit Kits

Exploit kits (EKs) became popular as an automated infection vector in 2006. They are primarily used to mass distribute commodity malware by exploiting unpatched/vulnerable systems in order to trigger a drive-by download. In simple terms, EKs attempt to detect a vulnerability in a browser-related application then exploit it to download and execute a malicious payload. The downloaded payloads vary across exploit kits and the campaigns that leverage them.

EKs can be rented from their creators through exploit-kits-as-a-service (EKaaS) for around \$900 USD per month¹⁴. EK activity has been relatively low for several quarters but is starting to increase as payloads shift from ransomware to banking trojans¹⁵. Exploit kits also continue to advance in terms of complexity and vulnerability coverage, as shown by the Purple Fox exploit kit. Purple Fox's latest updates included recent CVEs¹⁶ and rootkit capabilities used to avoid detection and hinder analysis¹⁷.

OFF-THE-SHELF THREATS

Remote Access

Cobalt Strike

Cobalt Strike is a fully featured and supported threat emulation software that is still under active development. In some cases, it may prove cheaper and faster than developing in-house tooling, with licensing starting at \$3,500 per year¹⁸. These factors have contributed to it becoming one of the most prevalent and favored tools among red teams and attackers¹⁹.

There have also been incidents where source code and cracked copies of Cobalt Strike were leaked. These copies were subsequently leveraged in malicious attacks on enterprises by a growing number of APT groups such as APT32, APT27, and APT29.

Cobalt Strike and Metasploit are the two most common penetration testing frameworks available on the market. A recent report²⁰ estimates that more than 25% of the malicious command and control (C2) servers deployed in 2020 rely on Cobalt Strike and Metasploit. Approximately 82% of all beacons analyzed by BlackBerry appear to come from leaked or cracked copies. The prolific use of these widely available copies makes it difficult to attribute their malicious activity to a specific group.

25%

of malicious C2 servers in 2020 rely on Cobalt Strike and Metasploit

82%

appear to come from leaked or cracked copies

Enumeration

AdFind/SharpHound

Adfind is a command line utility used to enumerate Active Directory for information such as:

- Computers in the domain
- Trust objects
- Domain controller FQDNs
- Users where a password is not required
- Other potentially useful pieces of information²¹

Adfind has been leveraged by APTs²² and commodity malware groups like “one”²³, the group behind Ryuk ransomware distribution. Threat actors use Adfind to gather information for further probing or moving laterally within an infected environment. SharpHound, the data collection component of BloodHound²⁴, is another Active Directory enumeration utility. It is used to map out potentially unseen relationships within a domain²⁵. Such mappings can provide an attacker with the shortest and sometimes easiest path to achieve Domain Admin privileges within an environment²⁶. SharpHound comes in multiple forms, including a DotNet compiled executable (.exe) file and a PowerShell script where the assembly has been obfuscated. BlackBerry has observed the use of both AdFind and SharpHound by malicious threat actors during 2020 and expect to see them again in 2021.

Lateral Movement

Mimikatz/LaZagne

Mimikatz is a widely used tool in the post-exploitation phase of an attack. It is used to aid lateral movement. Threat actors use Mimikatz to steal credentials from a compromised host and discover other credentials, allowing them to move laterally within the network environment²⁷. It was recently updated to include exploit code for CVE-2020-1472, the critical ZeroLogon privilege escalation vulnerability²⁸. The combination of Mimikatz and ZeroLogon on an unpatched system could prove devastating for an entire enterprise network²⁹.

Mimikatz has been a longstanding staple of the attacker toolkit. Given the popularity of Mimikatz, one can safely assume that most antivirus and endpoint detect and response products have built-in mechanisms to protect against or detect its usage. This creates the opportunity for the development of competing products for retrieving credentials from a system. One such alternative is LaZagne³⁰. LaZagne contains a Mimikatz-like module (pypykat³¹) but includes versions for Linux and Mac as well as Windows. It can also target software such as browsers, mail clients, and Wi-Fi configurations among others.

ATTACKS ON CRITICAL VERTICALS

With the Dark Net providing easy access to stolen credentials, off-the-shelf post-exploitation tools, and convenient RaaS solutions, attacks against critical infrastructure have become increasingly prevalent. Numerous phishing campaigns aimed at stealing login credentials targeted critical manufacturing, healthcare, energy services, and food supply sectors in 2020.

It's no surprise that in times of a global pandemic, healthcare and medical research are of primary interest to cyber criminals. During 2020, BlackBerry observed increased incidence of ransomware attacks against hospitals and healthcare providers. In most cases, the threat actors gained access to the victim's environment by hacking the victim's MSSP or obtaining valid RDP login credentials. The lateral movement, as well as data exfiltration, are often done with publicly available tools and customized PowerShell and batch scripts. Cobalt Strike is by far the most popular solution for establishing a foothold in target environments. Ransomware families seen in attacks against healthcare include Maze, Ryuk, Netwalker, and Sodinokibi.

Another pandemic-related threat to critical infrastructure are attacks targeting organizations developing COVID-19 vaccines. Campaigns started as early as April 2020 and are quite different from financially motivated ransomware incidents. These attacks are focused on

espionage and data exfiltration and are believed to be primarily sponsored by nation states. In July 2020, the United Kingdom's National Cyber Security Centre warned against large-scale phishing campaigns attributed to APT29 (aka CozyBear) targeting COVID-19 research facilities. Once credentials were obtained, the adversaries used WellMess and WellMail malware to steal data³².

According to IBM, another campaign, aimed at the vaccine transportation chain, started in September. It involved precisely targeted phishing emails sent to transportation organizations in a bid to steal information related to purchase and intended movement of the vaccine³³. AstraZeneca, the developer of one of the leading vaccine candidates, was targeted in November by suspected North Korean attackers. The adversaries, disguised as recruiters, were sending out malicious documents purporting to be job descriptions³⁴.



OS

CYBER THREATS



TOP MAC THREATS



Filecoder

Filecoder, aka FindZip or Patcher, is a notable ransomware family affecting MacOS. Unlike many other ransomware strains, this family seems to be more focused on destruction than generating revenue. Files are encrypted with a pseudo-randomly generated key and a ransom note is dropped to the desktop demanding payment to restore the encrypted data. However, during execution nothing is transmitted back to the threat actor. This means that if the victim pays the threat actor, they will receive no decryption assistance as the keys are not known by either party.

Samples of Filecoder were detected masquerading as a crack tool for popular software on torrent sites. This successful tactic underscores the importance of only downloading and running software from reputable sources and not blindly allowing execution from untrusted applications. Filecoder depends on *zip* functionality to perform the encryption. Luckily, a known plaintext attack on *zip*'s functionality can be used to decrypt the data without needing the generated encryption keys³⁵.

NukeSped

NukeSped was discovered as a trojan cryptocurrency application for MacOS in late 2019 and attributed to APT38/Lazarus³⁶. Attackers faked company information and a landing page to lend their campaign an air of legitimacy. The landing page also distributed the malicious application, based on research done by Patrick Wardle.

NukeSped capabilities include persistence via a launch daemon, system information gathering, and network connectivity to the threat actors for secondary attack stages. Later stages are presumed to be downloaded and executed in memory as an attempt to thwart detection. NukeSped is not signed, so Gatekeeper, by default, will warn the user and request permission to execute. This is another reminder to not install or run software from an untrusted source.

FinSpy

FinSpy, also known as FinFisher, is spyware created and sold by the German company FinFisher GmbH. It has been attributed to multiple attacks and privacy violations against human rights defenders according to Amnesty International³⁷. Campaigns using FinSpy have been used against citizens in countries such as Bahrain, Ethiopia, UAE, and Turkey. FinSpy contracts were also associated with previous Egyptian authorities.

The software can access private communications and data and record live audio and video directly from the infected device. MacOS variants of FinSpy exploit bugs in older versions of OSX or ask the user to allow elevated permissions if unsuccessful. C2 servers are used for communication between the victim device and the attacker to transfer data and initiate recording³⁸.

TOP MAC THREATS



EvilQuest

EvilQuest/ThiefQuest is a MacOS ransomware that was discovered in mid-2020. Ransomware is not as common on MacOS as some other operating systems, but it is becoming more prolific over time. EvilQuest ransomware has been found in illegitimate copies of MacOS and trojanized versions of other software.

Under normal conditions, MacOS Gatekeeper would prompt the user to confirm execution privileges, as the samples encountered were not signed. The malware also requests administrative privileges from the active user. EvilQuest uses a launch daemon to achieve persistence. The malware has remote code execution functionality so data such as user certificates and cryptocurrency wallets can be exfiltrated to the C2 server³⁹.

AppleJeus

AppleJeus is malware associated with the threat actor group APT38/Lazarus. It targets users involved in cryptocurrency trading. To boost the legitimacy of their operation, the attackers allegedly created a fake cryptocurrency trading platform offering download installers for both Windows OS and macOS. Running the installer gave the threat group access to the host system.

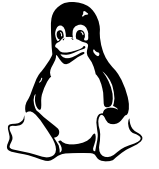
AppleJeus achieves persistence via a created launch daemon. Once running, the malware will gather basic system information and relay it to the C2 server. The C2 server will respond with tasks if certain conditions are met⁴⁰.

Dacls RAT

The Dacls remote access trojan (RAT) originally targeted Windows and Linux systems but a variant for MacOS was found in mid-2020. The malware is believed to be associated with the APT38/Lazarus threat group. Social engineering is a common attack vector for Lazarus and was used in this case as well. It is believed that users are infected by executing trojanized downloads that contain the malware.

Similar to other MacOS malware, Dacls RAT achieves persistence through the use of a launch agent. The RAT has C2 communication capability to execute commands remotely, perform file transfers and network scanning, and process enumeration and management⁴¹.

TOP LINUX THREATS



Mirai

Mirai is a prolific botnet that targets vulnerabilities in networking hardware like home routers and IoT devices such as Internet-connected cameras. It uses default credentials and general dictionary attacks to gain access to vulnerable devices based on various architectures.

The Mirai source code was made public in 2016 and has since seen numerous changes and additions as new variants are discovered in the wild. The original leaked code is still available on GitHub for research purposes⁴². The original code contains a range of IP addresses that are explicitly not valid during the target IP generation process. The U.S. Department of Defense, United States Postal Service, Hewlett-Packard, General Electric, and internal network ranges are specifically mentioned within the codebase⁴³. These government entities and corporations have been assigned large ranges of IPv4 space. For example, the whole of 56.0.0.0/8 is assigned to USPS⁴⁴.

Mirai is attributed to the widely covered DDoS attack on a top investigative journalist's blog, Krebs On Security. This attack broke records for DDoS traffic at the time⁴⁵. Mirai was also used for a DDoS attack on Dyn⁴⁶. The malware continues to be an active threat in 2020.

Gafgyt

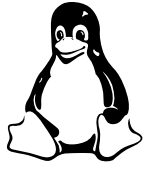
The Gafgyt botnet first appeared in 2014, targeting the ShellShock/Bashdoor vulnerability. The source code was publicly leaked, which led to many malware variants that target various devices like IP cameras and routers across numerous architectures. Gafgyt has also targeted video gaming services in addition to consumer networks such as Valve's Source Engine services and Fortnite⁴⁷.

Gafgyt attack methods and specific exploits have changed over the years as new builds are found, including variants discovered in 2020. This threat is also known as BASHLITE, qbot, and torlus⁴⁸. Gafgyt continues to be an active threat in 2020, a recurring theme as the family was also covered in the BlackBerry 2020 Threat Report.

Tsunami

Tsunami is also known as Muhstik, Radiation, Amnesia, and Kaiten⁴⁹. The Tsunami botnet is known for targeting IoT devices and communicating using the IRC protocol. Tsunami is part of the highly discussed Linux Mint distribution compromise that led to ISOs of the distribution to ship with the threat baked in⁵⁰. This threat utilizes vulnerabilities ranging from hardcoded admin credentials to those in content management systems such as Drupal⁵¹.

TOP LINUX THREATS



IPStorm

The IPStorm botnet was discovered in 2019. It is written in Golang, which uses the InterPlanetary File System (IPFS), a peer-to-peer (p2p) filesharing and networking system for communication. Communication may route through many legitimate peers between the threat actor and the intended target. This routing makes it difficult to differentiate malicious traffic as it is mixed with benign traffic throughout the IPFS network⁵².

This threat originally targeted Windows systems but has branched into supporting multiple architectures on Linux, including Android. Infection occurs by either brute forcing SSH credentials or, in the case of Android, looking for exposed debug functionality⁵³.

IPStorm was discovered by Intezer. On Linux, IPStorm issued numerous requests to the Steam API, a gaming service provided by Valve, querying possible stolen accounts on the service⁵⁴. Intezer also discovered evidence of devices infected with IPStorm being used to create fraudulent advertisement views⁵⁵.

WellMess

WellMess was first publicly referenced in 2018 by JPCert. It has evolved from initially targeting Windows machines to infecting Linux along with other communication protocols. The malware allows remote code execution and file transfers⁵⁶.

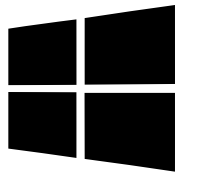
WellMess is associated with threat group APT29 by multiple sources, including the United Kingdom's National Cyber Security Centre, Canada's Communications Security Establishment, and the United States' National Security Agency. Also known as WellMail, this campaign targets organizations connected with the research and development of COVID-19 treatments. WellMess is written in Golang and utilizes multiple avenues of attack, including publicly known CVEs against software such as Citrix, Pulse Secure, FortiGate, and Zimbra⁵⁷.

FritzFrog

First discovered in January 2020, FritzFrog is written in Golang and has quickly become a notable botnet. FritzFrog targets SSH services and attempts to brute force credentials to gain access. Many botnets use common credential combinations around built-in accounts such as root, but FritzFrog uses a much larger dictionary to cast a wider net.

FritzFrog is unique in the sense that it does not rely on commonly used communication protocols, instead using a custom p2p implementation. Operations are also done completely in-memory, avoiding the use of the filesystem. In some cases, FritzFrog is also associated with Monero cryptominers⁵⁸.

TOP WINDOWS THREATS



BazarLoader

BazarLoader, otherwise known as KEGTAP, is a recently uncovered malware loader. It has been described by researchers as having close ties to the infamous Trickbot malware variant. The two threats share various similarities in codebase and infrastructure. First seen in April 2020, BazarLoader's name is derived from its use of EmerDNS blockchain domains for C2 communications, specifically the use of .bazar domains.

BazarLoader typically uses spam and phishing emails as an infection vector. Once downloaded to a machine, the malware attempts to connect to a C2 .bazar domain. Upon a successful check-in, the malware uses process injection techniques to attempt to run undetected in the address space of legitimate Windows processes.

As its name suggests, BazarLoader proceeds to sleep for a short time before attempting to download a malware payload from the attacker's C2. Cobalt Strike has been seen deployed in the wild within a BazarLoader attack chain; however, the payload may be anything of the attackers choosing. BazarLoader also uses heavy code obfuscation, stealthy installation, and a sophisticated C2 infrastructure, making it a severe threat to any company or user.

Astaroth

First spotted in the wild in 2017, Astaroth is an information-stealing malware variant that targeted Brazilian users. From its initial inception to the present day, it has evolved in sophistication and capabilities across numerous campaigns. Astaroth now targets users both in North America and Europe, and deploys measures to avoid detection from victims and security vendors alike.

Utilizing spam emails as its primary infection vector, Astaroth has refined its execution chain to employ a sophisticated multi-stage process that includes:

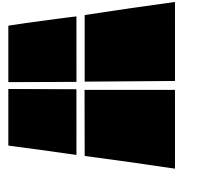
- Making use of malicious iframes
- Highly obfuscated JScript staged downloaders
- .lnk files to retrieve the malware payload once an unwitting user clicks an embedded link in the spam email

Upon infection, the malware uses various fileless techniques, injects into numerous legitimate Windows processes, and adopts the use of living-off-the-land tactics. The malware uses or abuses legitimate utilities that are already installed on a system such as "bitsadmin.exe". This hijacking of legitimate resources is an attempt to avoid suspicion and remain undetected on a victim host.

Later versions of Astaroth incorporated Alternate Data Stream (ADS) functionality and the abuse of different living-off-the-land binaries (LOLBins) such as "extexport.exe". It also included Facebook and YouTube within its attack life cycle, abusing these sites to send and store C2 configuration data as posts on user profiles. These new capabilities demonstrate that Astaroth is a continuously evolving and sophisticated threat. Information targeted by Astaroth includes financial data, sensitive browser data (passwords/credentials), SSH, and email credentials. Upon retrieval, the information is typically encrypted, then exfiltrated via an HTTPS POST to the attacker's C2 server.

Astaroth remains a sophisticated and prevalent threat by making use of heavy obfuscation, stealth, and living-off-the-land techniques. Astaroth's ability to steal a wide array of sensitive information and maintain a sophisticated C2 infrastructure makes it dangerous to companies and users today.

TOP WINDOWS THREATS



Bladabindi

First identified in 2012, Bladabindi, also known as njRAT, has gained popularity due to several tutorial videos available on YouTube and the builders being available on GitHub. This remote access trojan malware is especially popular among Middle Eastern threat actors.

The initial creators of Bladabindi are an underground attack group called Sparclyheason. Bladabindi can activate web cameras, log keystrokes, capture screenshots, steal passwords, execute remote commands, and more. The malware is written in .NET and consists of two main classes – kl and OK. The kl class is used for keylogging while the OK class has other Bladabindi RAT functionalities. The OK class also contains a hardcoded 32-character long string value consisting of lowercase letters and numbers, unique per sample.

This string value is used when malware installs itself at autostart for persistence under

```
'HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ab1c039a01d925ae481774f412396f5e'
```

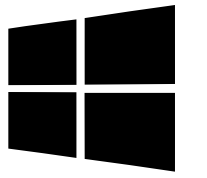
and

```
'HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\ab1c039a01d925ae481774f412396f5e'
```

with the value of path of stored malware under

```
%TEMP%, %APPDATA%, %USERPROFILE%,%ALLUSERSPROFILE%.
```

TOP WINDOWS THREATS



Cerber

The first variants of Cerber ransomware appeared in March 2016. The malware uses an RaaS model and is offered in Russian underground forums. Implementing Cerber via the RaaS model increases the number and reach of attacks. Cerber affiliates are responsible for finding and infecting victims while the developers take a commission of up to 40% of any ransom amounts collected.

During execution, Cerber will first check the country of the infected endpoint. If it finds this to be located in any of the following nations, it will terminate its execution and not encrypt the system:

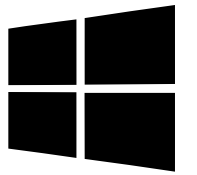
- Armenia
- Azerbaijan
- Belarus
- Georgia
- Kyrgyzstan
- Kazakhstan
- Moldova
- Russia
- Turkmenistan
- Tajikistan
- Ukraine
- Uzbekistan

Often, malware developers will avoid attacking endpoints within their own geographical region. This assists in limiting their exposure and avoids drawing the attention of local authorities. If the infected host passes the location check, Cerber creates a copy of itself in the victim's %APPDATA% folder under a random name chosen from the System32 directory. The malware scans all drives and begins its encryption process silently in the background using AES-256 and RSA encryption.

Cerber ensures no system backups are available and prevents the execution of antivirus applications and Windows security features. Files required for regular operations are encrypted, making the system unusable to the user. Early variants of the malware appended the file extension ".cerber" to encrypted files, although over time, other extensions have also been used.

When the encryption has successfully completed, a ransom message is displayed. The ransom is requested in bitcoin and, as an added incentive to pay, a time limit may be provided before the amount increases. Victims choosing to pay the ransom to retrieve their data have no guarantee the affiliate distributing Cerber will provide a decryption tool.

TOP WINDOWS THREATS



Emotet

Emotet is an advanced, modular banking trojan that primarily functions as a downloader or dropper of other banking trojans. It is a polymorphic threat, able to evade typical signature-based detection. It has several methods for maintaining persistence, including auto-start registry keys and services. It uses modular dynamic-link libraries (DLLs) to continuously evolve and update its capabilities.

Emotet is also virtual-machine-aware and can generate false indicators if run in a virtual environment. It is disseminated through malspam that uses branding familiar to the recipient. It has even been spread using the MS-ISAC name. The 2020 Emotet campaign distributed malspam in large quantities. Like many other threat actors, Emotet distributors took advantage of the COVID-19 global pandemic, which affected millions worldwide. The latest Emotet campaign sent a high volume of emails with subject lines like “COVID test results”, which contained a malicious link or PDF.

Initial infection occurs when a user opens or clicks the malicious download link, PDF, or macro-enabled Microsoft Word document. Once downloaded, Emotet establishes persistence and attempts to propagate through the local networks using incorporated spreader modules. Further details about recent advancements in Emotet appear later in this report.

Kwampirs

Kwampirs is a remote access trojan that targets supply chain software providers of critical industries. The malware made a resurgence in 2020 alongside the outbreak of COVID-19, which has left many industries, healthcare in particular, facing tough times. Attack groups deploying Kwampirs have been taking advantage of the vulnerabilities these industries are facing by attacking their supply chains. The attacks are having such a devastating effect that the FBI released multiple alerts to warn potentially impacted industries and services.

The Kwampirs RAT is a fully featured backdoor that uses a two-phase approach. The initial phase establishes a wide and persistent presence on the target network. In this initial phase, the trojan uses hidden admin shares to propagate via SMB port 445. The malware is modular and can download additional modules on the target. This occurs in the second phase where all C2 network traffic is carried out. Kwampirs uses HTTP GET requests on port 80 and includes the encrypted date in the Uniform Resource Identifier (URI).

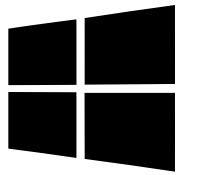
Ryuk

Since first appearing in August 2018, Ryuk has specifically targeted enterprise environments, similar to other ransomware families such as Samas and BitPaymer. Upon its release, researchers from Checkpoint conducted a code comparison between the initial versions of Ryuk and the Hermes ransomware variant. They discovered that the two threats were highly similar in nature. Researchers therefore concluded that Ryuk was, in fact, a derivative of the Hermes source code that has been steadily developed since its inception.

Hermes has always been considered commodity malware, meaning that it has been used by various threat actors and observed for sale on numerous underground forums. Ryuk, on the other hand, has been attributed to a Russian-based threat actor dubbed WIZARD SPIDER. Also, unlike Hermes, Ryuk has traditionally been used to target larger enterprise environments and organizations in attempts to obtain a high-ransom return.

One example occurred in June 2019, when the State of Florida paid over \$1,000,000 to bring the city’s systems back online. Affected entities included police, SCADA, and water-related systems. WIZARD SPIDER is also believed to be behind the Trickbot variant of banking malware. This may explain why Ryuk has recently been seen being deployed in a triple-threat scenario along with Trickbot and Emotet.

TOP WINDOWS THREATS



Smoke Loader

Smoke Loader, also known as Dofil, Sharik, and Smoke, was first discovered in 2011. It was advertised in forums as:

- A modular loader that could deliver up to 10 different executables
- Small in size
- Containing a password-grabbing module for email clients, FTP clients, browsers, IM clients, poker applications, and more
- Having functionality that can be expanded via plugins

Over the years, Smoke Loader has evolved many capabilities. It added a process injection method (mostly against explorer.exe) and the ability to drop other malware via weaponized documents. Later versions of this malware include anti-analysis and anti-debug checks to protect itself and detect any antivirus vendor presence.

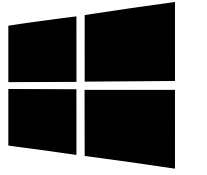
Trickbot

Trickbot is an advanced modular banking trojan that was first reported in 2016. It was originally designed to steal sensitive user content, including banking credentials and other personal data. The creators have since expanded its capabilities by adding new modules to evade detection efforts and enhance functionality. Some of the modules added facilitate VNC-base remote access, lateral movement, and the installation of a UEFI/BIOS firmware implant for persistence (as reported by AdvIntel and Eclipsium). The sophisticated firmware implant means Trickbot can survive even after reformatting the hard drive. Trickbot also developed into a platform-as-a-service, allowing it to deliver additional malware such as Ryuk and Conti Ransomware.

Trickbot is often distributed by Emotet spam trojan as a second-stage payload. It is also delivered via spam campaigns that capitalize on enticing subjects related to unpaid invoices, purchase orders, or other financial transactions. In 2020, Trickbot operators added COVID-19-related terms into their phishing and malspam lures. Like many other threat actors, Trickbot distributors took advantage of the COVID-19 global pandemic affecting millions worldwide. According to Microsoft's ATP data, Trickbot is the most prolific malware operation using COVID-19-themed lures.

Despite recent efforts by Microsoft and the FBI to disrupt Trickbot servers, this malware family still poses a serious threat. The threat actors behind this malware continued their operations, adding features and pushing new updates to make it more resilient against future takedowns.

TOP WINDOWS THREATS



Wacatac

Wacatac is a generic detection category for malware trojans that:

- Can be distributed through malicious emails as part of phishing campaigns
- Are dropped to a system by other malware
- Are unknowingly downloaded by users when browsing compromised websites
- Are launched under the mistaken belief it is a software patch or crack

Once on the system, the trojan can execute malicious activities. Examples include gathering personal and banking details, downloading additional malware payloads, providing remote access to the system, or adding the endpoint to a botnet.

The trojan usually copies itself into the user's startup folder or creates a registry key for persistent execution at every system boot. Also, it will often drop files to the %APPDATA% directory and may attempt to determine the victim system's IP address by connecting to myIPAddress.com.

Wacatac detection is sometimes associated with the ransomware DeathRansom because of the registry key created by this family:

```
HKEY_CURRENT_USER\SOFTWARE\Wacatac
```

Being a generic trojan detection, Wacatac is not associated with any specific threat group and has a broad range of non-specific trojan aliases.

CYBERSECURITY INSIGHTS



SECURING THE ELECTORAL PROCESS

On October 19, 2020, the U.S. charged six Russian military intelligence officers with conducting a series of high-profile cyber attacks⁵⁹. The alleged crimes were outlined in a 50-page indictment⁶⁰, and included:

- Attacks on Ukraine's power grid
- Compromising systems for the 2018 Winter Olympic Games
- Global NotPetya attacks
- Interference (hack-and-leak efforts) in the 2017 French elections

Likewise, Robert O'Brien, national security adviser, accused China of meddling during the run-up to the 2020 U.S. presidential election⁶¹. While electoral skullduggery between nation states is nothing new, minimizing foreign interference is a critical aspect of maintaining free and fair elections.

SECURING THE ELECTORAL PROCESS

Beyond the Ballot

Often, electronic voting systems are the focus of electoral security, but elections can be attacked through a number of different means. Consider the sheer number of smartphones, tablets, laptops, desktops, and other connected technology used by a political candidate and campaigns. Each application, device, and network used by this group offers threat actors a potential attack surface.

Likewise, like the general electorate, many policymakers and their staff are active on social media. Adversaries can collect considerable information from users' posts to help them tailor an effective attack strategy. General information people volunteer about themselves online may not seem potentially harmful, but it can be in the hands of trained threat actors.

For example, people post information on how busy, tired, or overwhelmed they feel. Threat actors can use this information to time their attack, knowing fatigued people are more prone to make mistakes. Users discuss issues, topics, and events that interest them. Adversaries can use this information to send targeted emails aligning with these interests to increase the likelihood users will interact with them. The amount of actionable information threat actors can access on social media pages is considerable, and includes⁶²:

- Video blogs revealing building layouts, equipment, team processes, secure areas, and whiteboard plans
- Team pictures revealing the hierarchy, membership, and interests of people within an organization, and often, their location

- Common complaints, concerns, or disputes in an organization that can later be used as a lure in a phishing email

Policymakers and their teams are vulnerable targets for having their social media accounts mined for exploitable information. While not as dramatic as blatantly switching votes in an election, compromised political parties and operatives can represent a real danger to election security.

Email is another weak point for election security. The Domain-based Message Authentication, Reporting, and Conformance (DMARC)⁶³ standard is used to verify that an email came from a specific sender. Email verification is an important tool for fighting election-year misinformation, yet only 15% of campaigns and PACS



used DMARC in 2020⁶⁴. At the beginning of 2020, a full 95% of the largest voting counties in the U.S. were vulnerable to phishing attacks and forged emails.

What Can Be Done?

Election security can be improved by modifying personal behaviors, and wisely implementing effective technical countermeasures. Users can improve election security by limiting the information they share on social media and interacting with others only through known and trusted channels. For example, communicating with a government organization through their official website is more secure than responding to random emails allegedly coming from them. Users can also practice good security hygiene with work and personal devices while limiting the amount of technology with access to sensitive information.

Artificial intelligence (AI) can play a strong role in verifying user identities. Behavioral analysis, facial recognition, location analysis, and biometric monitoring all offer AI actionable data sets for validating user identity. AI can perform simple, less intrusive functions to prevent voter fraud like authenticating signatures⁶⁵. It can also play a role protecting elections from foreign interference on the Internet, when used by organizations to identify and restrict disinformation campaigns⁶⁶.

BAHAMUT

BAHAMUT is an active threat group investigated extensively by BlackBerry threat researchers in 2020⁶⁷. The threat group traffics in fake news sites, personas, and social media accounts. They also had dozens of malicious apps hosted on the App Store™ and Google Play™ store. BAHAMUT is known to researchers worldwide under many names, including HDEVEL, WINDSHIFT, URPAGE, and THE WHITE COMPANY.

During their investigation, BlackBerry researchers observed BAHAMUT operations against government officials and industry leaders in India, the Emirates, and Saudi Arabia. Advocates for Sikh separatism and organizations supporting human rights causes in the Middle East also suffered attacks from BAHAMUT. The threat group has demonstrated zero-day threat capabilities, indicating it has access to at least one zero-day developer. One particular zero-day exploit targeted InPage, a word processor popular in Urdu, Arabic, Persian-speaking countries, and the major newspapers in Pakistan and India.

BAHAMUT works hard to cover its tracks, ensuring its activities remain difficult to detect or attribute. It uses tools created by other threat groups (or publicly available alternatives) and keeps its campaigns, network infrastructure, and phishing tools separated. BAHAMUT may obscure its activity by imitating the same TTPs popularized by other threat groups. Backdoors and exploit shellcode written by BAHAMUT often includes anti-analysis features. When its activities are detected, the threat group quickly changes tactics and corrects any missteps leading to its exposure.

BAHAMUT

Former Targets of BAHAMUT

The early targets of BAHAMUT were chronicled by Collin Anderson and Claudio Guarnieri on the investigative journalism site Bellingcat in June 2017. Their research indicates the threat group initially targeted individuals associated with the political, economic, and social sectors in the Middle East. These early targets included:

- Iranian women's rights activists
- Turkish government officials
- Saudi Aramco
- A Europe-based human rights organization
- People connected to Qatar's domestic and international politics
- Egypt-focused media and foreign press, including individuals previously imprisoned in the country
- Multiple Middle Eastern human rights NGOs and local activists
- The Union of Arab Banks
- The Prime Minister's Court of Bahrain

Other threat researchers, calling BAHAMUT by different names, observed the group selecting targets in South Asia, particularly in India and Pakistan. Some researchers report witnessing BAHAMUT activity in China and northern and eastern Europe as well. These cases show the threat group's tendency to target individuals rather than organizations. The Bellingcat documents suggest that BAHAMUT may act as a hacker-for-hire operation, given the vast diversity of specific targets.

Current Targets of BAHAMUT

BlackBerry research shows that South Asia and the Persian Gulf are the two regions most at-risk from current BAHAMUT activity. The group's phishing infrastructure remains focused on credential harvesting from popular sites like Google™, Microsoft®, Yahoo!®, and Telegram. Chinese sites Sina, QQ, 126, and 163 have also attracted BAHAMUT's attention. BAHAMUT seems to largely avoid targets in the United States.

BAHAMUT recently targeted seven ministries and agencies of Saudi Arabia that were connected with monetary and financial policy. Government agencies dealing with foreign policy and defense were also targeted in the Emirates, Qatar, Bahrain, and Kuwait. The threat group's mobile phone strategy, consisting of fake app creation, targets a general audience in the Middle East. However, the fake mobile apps created for South Asians are more political and target groups like Sikhs for Justice, and Islamist groups in the Kashmir region, like Jamaat-ul-Islami and Jaish-e-Mohammad.

BAHAMUT Synopsis

BAHAMUT is a well-funded, technically adept, highly secretive, and effective threat group. The group's obfuscation capabilities and mimicry of other's techniques has made it difficult to identify and track. BlackBerry researchers, through exhaustive investigation, have concluded that this group is also known by the following names:

- "InPage" threat actor described by Kaspersky
- The group described in Cisco Talos' MDM blog posts
- WINDSHIFT5 as described by Darkmatter
- URPAGE6 as described by Trend Micro
- THE WHITE COMPANY as described by Cylance

For a deep dive into the tactics, targets, and activities of this threat group, read [BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps](#) [↗](#).

BAHAMUT's targeting is all over the map, which makes it difficult to concoct a single victimology. BAHAMUT appears to be not only well-funded and well-resourced, but also well-versed in security research and the cognitive biases analysts often possess. //

EMOTET: THE EVOLVING THREAT

Emotet is an evolving threat that has been terrorizing systems since 2014⁶⁸. The earliest versions of Emotet functioned as a banking trojan, performing man-in-the-browser attacks to steal credentials⁶⁹. These early versions focused on targets in Germany and Austria and featured malicious attachments created to look like invoices or other financial documents⁷⁰. Following its appearance and a few months of malicious activity, Emotet attacks declined until an updated variant emerged in 2015⁷¹. Emotet is designed to avoid attacking Russian-speaking countries⁷², which leads many researchers to believe it originates from Russia.

*...among the most
costly and destructive
malware affecting
SLTT governments.*

US-CERT

EMOTET: THE EVOLVING THREAT

Regular Updates

Emotet has received numerous updates over the years from a highly capable team of threat actors. These changes include the ability to detect virtual machines, transfer funds directly to attackers, deploy anti-analysis techniques, and incorporate a Windows API component⁷³. In 2017, Emotet transitioned to a more open and modular threat⁷⁴ and the main banking-based module was removed. By 2018, the United States Computer Emergency Readiness Team (US-CERT) recognized Emotet as *"...among the most costly and destructive malware affecting SLTT (state, local, tribal, and territorial) governments"*⁷⁵.

Major updates had occurred to Emotet by 2019, making it an advanced attack platform capable of delivering other threats like Trickbot and Ryuk⁷⁶. This multi-year transformation from banking trojan to global botnet allowed the threat actors behind Emotet to monetize it as malware-as-a-service⁷⁷. Emotet became the primary distributor of botnet delivered payloads, accounting for 61% of total malicious payloads by March 2019⁷⁸.

Emotet in 2020

The threat actors behind Emotet have taken periodic breaks from activity since the threat first emerged in 2014. In 2020, Emotet entered a period of inactivity ranging from February 7th to July 17th⁷⁹ before resuming in September. The 2020 version of Emotet arrived with two notable new capabilities and one unexpected flaw.

The first noteworthy Emotet update allows the malware to perform Wi-Fi brute force attacks and device infection⁸⁰. Previously, Emotet spread through two attack vectors, malspam and infected networks. With the Wi-Fi brute force upgrade, Emotet can propagate through insecure wireless networks and connected devices. While this new capability was not discovered until January 2020, the timestamp on the Wi-Fi spreading binary is set to April 16, 2018.

The second Emotet upgrade implements a tactic called hash-busting that acts as a countermeasure to malware identification and blacklisting. In the past, the Emotet loader could be identified by its unique file hash and preemptively shut down. Using hash-busting, in this case by adding 64 bytes of random data to the loader, each

Emotet infection has a unique file hash ID. This effectively counters blacklisting, as no two infections will be identical, and previously discovered Emotet loaders can easily be updated with new IDs.

The 2020 Emotet update also contained some good news for threat researchers, a design flaw that functioned as a kill-switch for the malware. The same mechanism used by Emotet to implement hash-busting was repurposed by threat researchers to stop the malware from running. Researchers, using the random file name generation function of Emotet could reset the malware's filename to ".exe", causing it to malfunction⁸¹. This tactic protected systems from Emotet infections from February 6, 2020 until August 6, 2020, when a new malware patch was released.

CONNECTED VEHICLES

Connected vehicles, which can contain over 100 independently developed components, are difficult to secure due to the multiple vendors involved in their assembly⁸². The sheer number of international entities participating in the automotive supply chain make enforcing common cybersecurity criterion extremely challenging.

Modern vehicles rely on multiple on-board computers to perform everything from critical system functions to navigation and entertainment. These advancements force car manufacturers to become experts in integrating and developing software⁸³. Vehicles are increasingly connecting to the Internet as well, with an estimated 280 million on-road automobiles currently Internet-connected⁸⁴. These factors set the stage for a crisis, automobiles becoming increasingly interconnected while auto manufacturers scramble to find ways to secure vehicle systems⁸⁵.

Until effective cybersecurity protocols and procedures are incorporated into the design and manufacture of vehicles, modern automobiles are effectively insecure networks. //



CONNECTED VEHICLES

Common Connected Vehicle Vulnerabilities

Connected vehicles are susceptible to cyber attacks ranging from simple data theft to highly advanced system hijacking. Some common vulnerabilities and attack vectors include:

- Hijacking electronic control units (ECU) to disrupt braking, steering, and engine operation⁸⁶
- Vehicle compromise through a paired smartphone⁸⁷
- Vehicle-to-Everything (V2X) and Vehicle-to-Vehicle (V2V) communication vulnerabilities⁸⁸
- Unintentional data exposure from previously paired devices⁸⁹
- Over-exposure of personal data (shared with OEMs, rental companies, car manufacturer, etc.)⁹⁰
- Vehicle vulnerability related to previous owners/renters⁹¹
- Reliance on network connectivity for functionality⁹²

Securing vehicles from cyber threats becomes increasingly difficult with every additional network connection, electronic component, and software-driven system. Until effective cybersecurity protocols and procedures are incorporated into the design and manufacture of vehicles, modern automobiles are effectively insecure networks.

The United Nations Gets Involved

The United Nations Economic Commission for Europe (UNECE) approved vehicle cybersecurity regulation WP.29 on June 25, 2020⁹³. This regulation outlines cybersecurity processes and measures that automobile manufacturers must meet to achieve vehicle type approval from UNECE. The UNECE standards apply to “contracting parties”, which includes many E.U. countries, China, Japan, and Korea⁹⁴. The new standards require automakers to⁹⁵:

- Make efforts to manage vehicle cyber risks
- Detect and respond to cybersecurity events across vehicle fleets
- Design systems to be secure throughout the supply and value chains
- Provide secure software updates to on-board systems for the lifetime of the vehicle

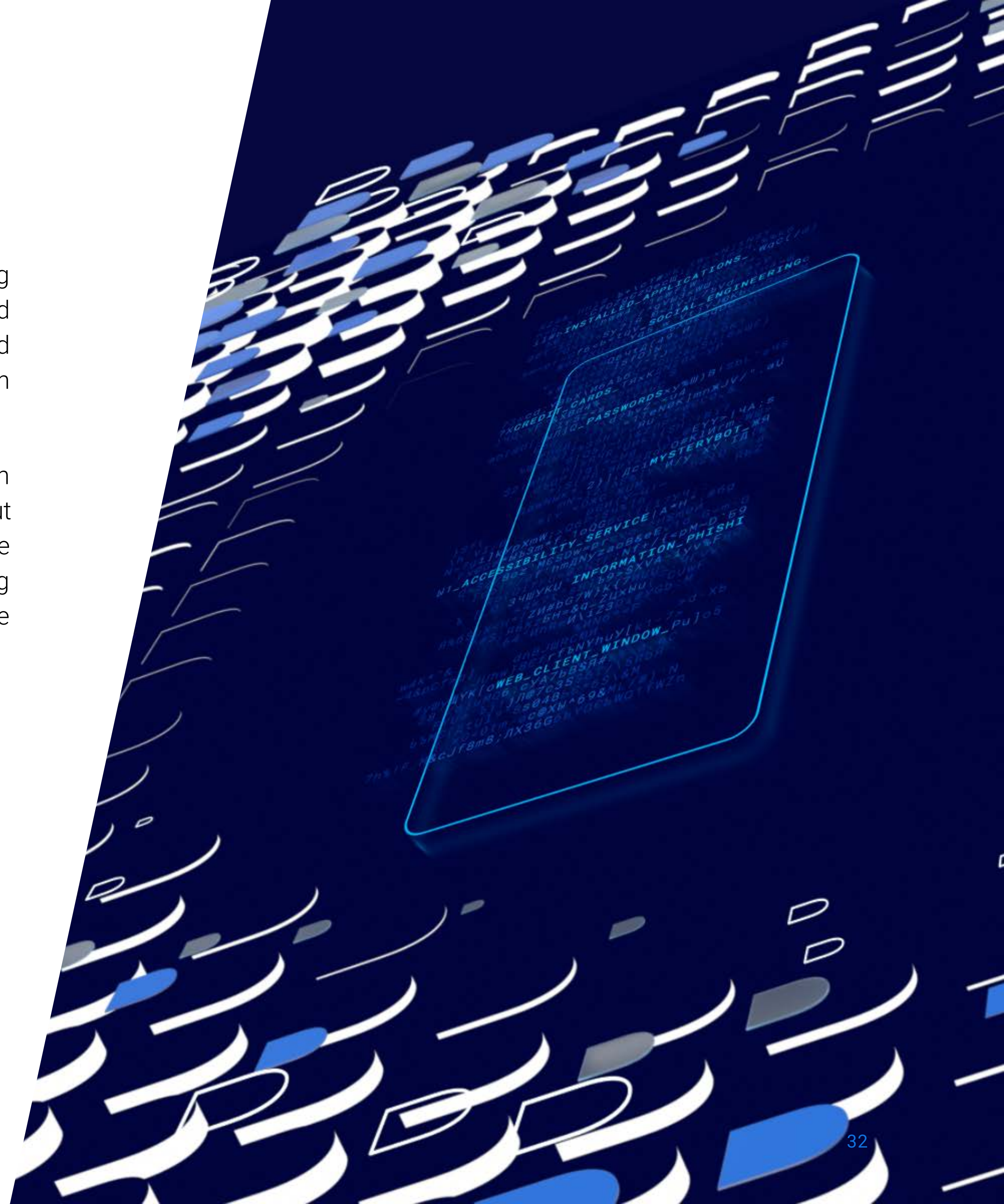
Vehicles that do not comply with these guidelines will not be approved for sale by UNECE.

The WP.29 regulations do not instruct automakers on how to implement cybersecurity into their processes. This means auto makers and OEM manufacturers will have to work together to find ways to comply with the regulation. Major industry players are working closely with the standards organization to develop cybersecurity standards, ISO 21434, which takes WP.29 regulations to an implementation level. While it is encouraging to see the auto industry embracing cybersecurity, the requirement for WP.29-compliant vehicles will not be enforced until July 2024⁹⁶. This delay leaves threat actors years to operate in the largely unregulated and insecure space of connected vehicles.

MOBILE OVERLAY ATTACK LIFECYCLE

Social engineering continues to be a highly effective means for stealing payment and access information. Presented within the context of an installed application, a prompt for credit card or passwords using a well-designed form often yields success for attackers. This trick works especially well when timed to coincide with application launch.

The theory is simple: present a credential or payment request at a time when the user is interacting with a target application. The prompt doesn't seem out of place or unexpected. The user dutifully enters the information because they believe it's necessary for the application to function correctly. Re-entering payment details into your favorite ride-sharing app, as it loads, when you're late for a meeting clearly plays to the attackers' advantage.



MOBILE OVERLAY ATTACK LIFECYCLE

Monitoring the foreground window against a list of targets is made possible through different methods. The most common and battery-friendly is via functions provided by the Accessibility Service (AS). The AS is a native function of Android designed to assist users with visual, hearing, and other related disabilities. A related method for timing an overlay attack leverages the foreground time or last used counters provided by the Android UsageStats service. While less battery-friendly, owing to the need to poll, this alternative approach still gives sufficient resolution to pop-up a request to an unsuspecting user. The Mysterybot information stealer employed this technique in 2018.

A prerequisite to using features of the AS is the `BIND_ACCESSIBILITY_SERVICE` permission, which, in addition to a long list of other malware-helpful features, allows an application to listen for changes in the foreground activity. When a foreground transition occurs, the malware is notified, and the package name of the new activity is queried against an internal list. If a match is found, the malicious overlay is shown to the user.

The accessibility service can permit an application to interact with activity controls (clicking buttons, entering text into fields, etc.). If a malicious application requires additional permissions, it can submit a request to the OS and then automatically click the OK button on-screen. This process occurs without any user involvement.

Information gathering overlays are composed of web content: a mix of HTML and/or JavaScript, rendered in a top-most WebClient window in front of the target application. The Android WebView class provides the necessary functions: *"A WebView is useful when you need increased control over the UI and advanced configuration options that will allow you to embed web pages in a specially-designed environment for your app."*

In-the-wild families that have, or continue to use overlay attacks, center most heavily around banking and information stealing malware: Anubis, Ginp, Cerberus, EventBot, and Marcher. Bank authentication details or payment card information for several apps specific to different countries is featured prominently amongst the activities of the Android malware community.

Google has announced forthcoming changes to the AS in Android 10 ("Q"), specifically deprecating the overlay feature. In addition, permissions for the AS will be automatically revoked after 30 seconds. While these changes are welcome, it's unlikely to have any impact on existing handsets that manufacturers have forgotten. Refusing to back-port security fixes entices users into upgrading.

The most effective means of defending against overlay attacks is to:

- Prevent installation of apps from sources other than the Google Play store
- Limit installation of apps that are not deemed essential
- Upgrade to the latest Android version
- Educate users on the methods employed by attackers targeting Android to steal valuable information



1/ Hijack Accessibility Service (AS) and leverage usage stats to figure out an optimal attack time



2/ Take advantage of user distraction and hurried behavior.



3/ Prompt user to enter credit card or password through false app overlay

THE YEAR IN RANSOMWARE

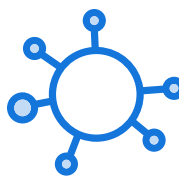
BlackBerry research has identified several notable ransomware threat trends in 2020, including:



A distinct shift from widespread, indiscriminate distribution to highly targeted campaigns often deployed via compromised managed security service providers (MSSPs)⁹⁷.



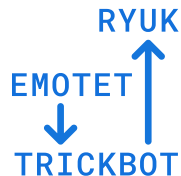
RaaS shifting to a more private model, where access to vetted affiliates is granted in exchange for sensitive information or for an agreed cut from the proceedings. Access could include an established foothold to compromised MSSPs, corporate networks, and/or government networks.



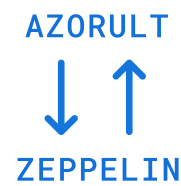
Increased collaboration and information sharing between ransomware threat actors and other threat groups, like those behind Emotet, Trickbot, and Azorult.



Exfiltration of data prior to, or during, the ransomware encryption process. This enables attackers to blackmail victims with the threat of exposing their sensitive data on public forums should they fail to pay the ransom in a timely manner. Additionally, General Data Protection Regulation (GDPR) in Europe requires companies to report any data breach. This can pressure companies to decide between paying a hefty regulatory fee or the ransom.



Ryuk collaboration with Trickbot and Emotet. This triple threat executes with Emotet dropping Trickbot on the host system to steal data. Trickbot then downloads Ryuk to perform ransomware operations.



Zeppelin collaboration with Azorult. Zeppelin ransomware can encrypt a system and install Azorult spyware to steal credentials, files, and other data.

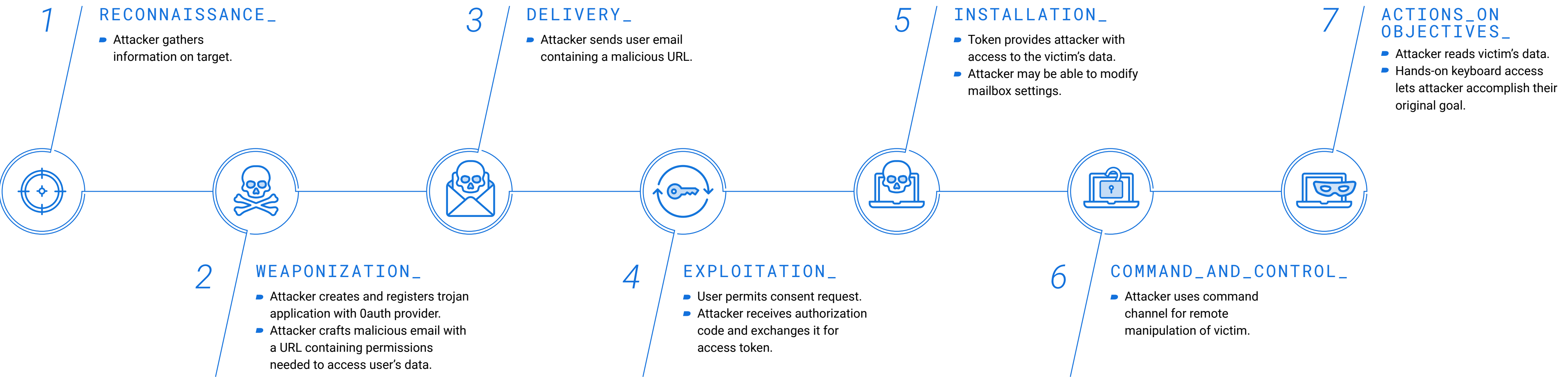
THE YEAR IN SPEAR PHISHING AND CREDENTIAL THEFT

BlackBerry research has identified several notable spear phishing and credential theft threat trends in 2020, including:

- The pandemic dramatically changed corporate working culture. Users shifted to working from home. Businesses had to scale up services to support operations and collaborations across the enterprise.
 - Remote working presented an opportunity for cyber criminals to exploit the new workplace reality with phishing attacks. Data from the Anti-Phishing Working Group showed that the number of phishing campaigns has grown since March 2020⁹⁸. The average wire transfer amount requested during a
- business email compromise attack is estimated to be \$48,000 in Q3 2020.

 - Software-as-a-service (SaaS) application and Webmail remained the most targeted services for phishing attacks, dominating others throughout the year. Financial and payment sectors ranked in the second and third positions⁹⁹.
 - A particularly interesting technique that drew BlackBerry researchers' attention was the use of trojanized applications to steal OAuth access tokens. Dubbed consent phishing,
- and discovered in the wild in December 2019¹⁰⁰, these campaigns provide an attacker a means to bypass multifactor authentication (MFA). Threat actors first trick users into providing permissions to a malicious application. The application then accesses the user's cloud data without using their username and password^{101 102 103}. This technique allows attackers to bypass traditional credential phishing defences and malware signatures.

Figure 1 illustrates a typical consent phishing attack lifecycle using the Lockheed Martin cyber kill-chain:



DEEFAKE THREAT ACTIVITY

One of the first cases of deepfake weaponization in the workplace was discovered last year. A senior official was tricked into transferring money after he received a call from a fraudster who impersonated the CEO's voice using deepfakes¹⁰⁴. This year, COVID-19 forced the corporate world to quickly pivot to providing secure remote connectivity for their workforce. As a result, cyber criminals rushed to weaponize deepfakes within the corporate world. In addition, primitive misinformation techniques like GIFs, photoshops, and face swaps continue to provide a simple and effective way for malicious actors to deceive users.

Findings this past year showed that a majority of deepfake activities were found within the entertainment industry in the form of non-consensual adult media¹⁰⁵. Researchers also discovered several underground forums selling deepfake services with more actors seeking ways to monetize this technology¹⁰⁶. Perhaps one of the most publicized weaponizations of this technology was centered around supporting disinformation campaigns. In April 2020, a deepfake video of the Belgian Prime Minister linking the cause of the pandemic to environmental damage was released¹⁰⁷.

In August 2020, Facebook removed 1,500 ads and 900 pages related to a site called Peace Data that promoted conspiracy theories to influence U.S. voters. Some editors of this site had deepfake profile pictures¹⁰⁸.

The bulk of attacks this year have largely focused on phishing, ransomware, hacking, etc. As normalcy returns around the world, threat actors may look towards increasing the weaponization of deepfake technology in the workplace, especially around facilitating sextortion campaigns.

CYBERSECURITY/DATA PRIVACY LEGISLATIVE AND REGULATORY FORECAST

UNITED STATES

If Democrat leadership holds true to historical tendencies, the Biden Administration and Democrat-controlled Congress could very well herald a more regulatory-friendly political environment in the U.S. Democrats historically have leaned toward increased federal regulation, and it is likely that the Biden Administration may do the same on cybersecurity and data privacy matters, especially in light of SolarWinds. It also is anticipated that the Biden Administration may support certain laws and regulations designed to bolster cybersecurity in the U.S. that were enacted under President Trump's leadership.

Cybersecurity

Congress and the Biden Administration are almost certain to introduce legislation and regulations to respond to the massive December 2020 SolarWinds attack. This attack included the networks of numerous federal agencies¹⁰⁹. We expect the introduction of federal bills and proposed rules designed to strengthen security and prevent a similar breach. New laws and regulations designed to better secure artificial intelligence (i.e., AI in vehicles), IoT devices, broadband, and infrastructure are also feasible.

Several newly enacted cyber provisions recommended by the U.S. Cyberspace Solarium Commission take effect in 2021, including:

- A National Cyber Director in the White House who will provide centralized leadership on currently disparate federal cyber-related mandates and policies. This person could also lead development of a National Cybersecurity Strategy.
- The Cybersecurity and Infrastructure Security Agency (CISA) will perform threat hunting identification on federal networks.
- An effort to bolster cybersecurity threat and information sharing and explore/study how best to secure connected cities in 2021.

CYBERSECURITY/DATA PRIVACY LEGISLATIVE AND REGULATORY FORECAST

Data Privacy

U.S. Federal

The partisan battle over federal data privacy legislation that picked up steam in 2020 may finally result in a federal law in the 2021-22 Congress. The most contentious issues Congress needs to resolve include:

- *Enforcement:* Democrats generally favor a private right of action, pursuant to which an individual could bring a suit (either individually, as part of a class action, or via a state attorney general), to hold technology companies accountable on data protection. Republicans prefer enforcement by a federal agency and state attorney general, because companies could go bankrupt fighting non-meritorious claims.
- *Federal pre-emption:* Republicans in Congress have generally supported a federal law that pre-empts state laws; they want to pre-empt state laws such as the California Consumer Privacy Act (CCPA). Their concern is there could be a patchwork of state laws and a new federal law with which companies must comply. Democrats, especially many in California, not surprisingly oppose federal pre-emption of state laws like the CCPA. They argue states should be able to raise the bar on privacy and consumer protection as high as they wish.
- The Federal Trade Commission (FTC), which enforces consumer protection, including privacy matters, may be given stronger enforcement and/or rulemaking authority by Congress.

U.S. State

Several states, including Washington, Maryland, Texas, and North Dakota, may follow California, Nevada, and Maine's leads and enact data protection laws in 2021. Most state privacy laws – and the bills nearing passage – give consumers greater control over the use of their personal information. The CCPA, for example, gives consumers the right to opt-out of certain data collection and to delete personal information collected, with some exceptions.

CYBERSECURITY/DATA PRIVACY LEGISLATIVE AND REGULATORY FORECAST

CANADA

On June 20, 2019, millions of Canadians with accounts in the Desjardins Credit Union (the largest in Canada) woke up to news that their personal information had been breached. Compromised information included names, addresses, birthdates, social insurance numbers, email address, and information about transaction habits. At the time, the Desjardins Group indicated that the breach affected around 2.7 million people¹¹⁰ and 173,000 businesses. Fast-forward to December 14, 2020, the Office of the Privacy Commissioner of Canada (OPC) updated the number affected in a detailed report¹¹¹.

The breach actually impacted nearly 9.7 million Canadians, a quarter of Canada's entire population. The OPC report¹¹² found Desjardins "did not demonstrate the appropriate level of attention required to protect the sensitive personal information entrusted to its care". The Privacy Commissioner called out Desjardins for failing to put in place adequate security measures to prevent this breach. The data compromise occurred over more than a two-year period before Desjardins even became aware of it.

The increasing scale, scope, and impact of privacy breaches, combined with reliance on digital technologies in today's data-driven economy, has ushered in a new era for cybersecurity and privacy legislation. Canada is set to modernize its aging privacy protection framework for both private and public sector organizations in 2021. Changes begin with the Consumer Privacy Protection Act¹¹³, which was introduced to Parliament by the Liberal government on November 17, 2020.

CYBERSECURITY/DATA PRIVACY LEGISLATIVE AND REGULATORY FORECAST

CANADA

The proposed Consumer Privacy Protection Act, which governs private sector organizations, includes some of the most severe penalties for privacy breaches in the G7. Companies failing to comply with the legislation could face monetary penalties of up to 5% of their revenue, or CA \$25 million, whichever is greater. The new legislation, which would come into force 18 to 24 months after it is passed into law, mirrors Europe's GDPR.

Under the legislation, companies are required to:

- Obtain consent from customers using plain language
- Provide greater transparency on how their data is being used
- Enable data portability and interoperability
- Provide Canadians with the ability to demand that their information be destroyed

The legislation also proposes to give the OPC broad powers, including the ability to force compliance from an organization. If adopted, Canada will have privacy legislation with teeth that forces companies to enact organizational and cybersecurity measures that adequately safeguard personal information. Accompanying this legislation will be the modernization of the public sector privacy law, the Privacy Act¹¹⁴. This law, which has not been updated since 1983, is expected to mirror the proposed Consumer Privacy

Protection Act. Together, they will raise the bar for privacy and cybersecurity in Canada.

Another area of increasing concern and focus in 2021, is Canada's aging critical infrastructure strategy and policies. Canada's critical infrastructure strategy¹¹⁵ has not been updated since 2009 and is ill-prepared to deal with today's cyber-based threats. As Canada looks to update its critical infrastructure strategy it should consider:

- Elevating the importance of cybersecurity across critical infrastructure
- Streamlining authorities and breaking down current administrative and bureaucratic barriers that could prevent the Canadian Government from detecting and responding to threats in a timely manner
- Developing a business continuity plan for the economy to promote national resilience if/when a cyber attack was to cause distress to critical infrastructure

Overall, 2021 is likely to see massive investments in cybersecurity infrastructure, technologies, and relevant legislation made by private and public sector entities in Canada. Canadians realize and understand the importance of safeguarding critical infrastructure and information, and how important privacy and cybersecurity are to a nation's economic and social well-being.

CYBERSECURITY, CRISES, AND COVID-19

The COVID-19 pandemic may be the crisis of a generation, but for threat actors, it simply presented an opportunity to capitalize on global chaos. As workers transitioned to home offices and businesses struggled to adjust their operations, cyber attacks spiked by 63%¹¹⁶.

The pandemic forced organizations to adapt to massive shifts in the workplace, supply chain, and consumer behavior while creating countless new attack vectors for adversaries. Attackers quickly tailored their efforts to exploit the new vulnerabilities created by COVID-19 by¹¹⁷:

- Conducting phishing and SMS phishing campaigns featuring COVID-19 or coronavirus-related terminology as a lure
- Registering domain names with titles or wording related to COVID-19
- Distributing malware by using COVID-19 or coronavirus-related terminology as a lure
- Attacking rapidly deployed remote access infrastructure
- Creating malicious mobile apps using COVID-19 or coronavirus-related terminology as a lure¹¹⁸
- Orchestrating COVID-19 stimulus-package¹¹⁹ and unemployment¹²⁰ scams

The COVID-19 pandemic has been globally disruptive, rewarding cyber attackers who have honed their tactics by exploiting smaller disasters over time. For example, in 2017, threat actors exploited Hurricane Harvey hitting Texas by creating malicious websites, phishing campaigns, and setting up fake charities¹²¹. In 2005, similar scams were performed in the wake of Hurricane Katrina¹²². While every unforeseen disaster sends professional organizations scrambling for solutions, threat actors can merely adjust their battle-tested tactics to reflect the new circumstances.

Cyber attacks
in 2020 spiked by

63%

CYBERSECURITY, CRISES, AND COVID-19

Securing Remote Infrastructure and Mobile Technology

Cybersecurity risks skyrocketed when COVID-19 forced workers to transition to home offices and children to remote learning environments¹²³. By March 2020, coronavirus-themed campaigns and attacks were well underway¹²⁴. These attacks began so quickly at the beginning of the outbreak that the World Health Organization released a statement warning of imposters using the organization's name¹²⁵.

Today, organizations have had roughly a year to adapt to changes caused by COVID-19. By now, businesses should be transitioning from their initial emergency response measures to a permanent long-term strategy for incorporating remote workers. A successful plan for accommodating remote and mobile workers should include:

- Maintaining employee productivity and user experience from any location
- Keeping both employee and organizational data secure at all times
- Maintaining regulatory compliance while enacting BYOD policies and allowing employees to work from remote locations

The steps seem simple, but each device, software app, and location added to the infrastructure exponentially increases its complexity. An estimated ten-fold increase¹²⁶ in work from home employees also represents an increase of routers, smartphones, mobile devices, and personal PCs handling company data. This puts companies in the difficult position of no longer having to worry about the security of one network, but thousands.

VPNs felt an enormous strain as some vendors reported usage increases of 165% in a month¹²⁷. Increased VPN usage from remote workers introduces new security risks, as all protected data is funneled to a single location, the provider's company. Incorrectly configured and/or vulnerable VPNs can expose remote employees who believe themselves secure to potential cyber attacks¹²⁸.

Vulnerabilities specific to VPN and remote communications were not the only new cybersecurity risks facing companies. Many home-based employees use personal or BYOD technology to assist with their job responsibilities. Ensuring employee's personal devices are updated and secure is a Herculean task. Confirming that the software and third-party apps on personal devices are also secure and up to date is an exercise in futility.

CYBERSECURITY, CRISES, AND COVID-19

The Zero Trust Solution

Zero Trust, as the name implies, is a security model where everything inside or outside an organization is initially treated as a threat. Nothing is granted access to organizational resources until it builds (and maintains) trust. The Zero Trust philosophy is attributed to John Kindervag, a former principal analyst at Forrester Research Inc., who coined the term in 2010¹²⁹. This framework solves the problem of securing every location and device used by remote employees by assuming they are untrusted by default.

Employees and new devices can connect to business infrastructure, but until they perform steps establishing their trustworthiness, their access is safely limited. Trust (and greater access) can be granted through a series of quick, non-intrusive measures commonly used today: two-factor authentication, security questions, etc. Once necessary access is granted, the user and connected device(s) are continuously monitored to ensure nothing suspicious occurs. The process sounds like it would be intrusive and resource-intensive, but AI makes achieving an almost frictionless Zero Trust security posture possible¹³⁰.

Ensuring that third-party apps and OEM software on BYOD devices is secure is another monumental task achievable through a Zero Trust framework. Work resources are relatively easy to monitor and protect within the business environment, but what happens when they are transferred to insecure BYOD devices? Implementing a secure gateway with IP layer security optimized for mobile and low-power devices can protect employee browsing and internal communications. Devices using the gateway can be sheltered from malicious URLs, dangerous apps, and phishing campaigns.

Disasters, both natural and manmade, inevitably place a heavy burden upon organizations while creating opportunities for malicious actors. Businesses, however, do not have to operate at a perpetual disadvantage. Implementing a Zero Trust framework for remote workers and BYOD devices can eliminate or reduce many successful tactics threat actors deploy in times of crisis.

CRITICAL EVENT MANAGEMENT FOR A SAFE AND SECURE OPERATING ENVIRONMENT

As countries tackle the challenge to create smart cities, data collection and protection becomes important for better managing a municipality's assets, resources, and services. Public utilities, traffic management networks, community facilities, and essential services will see improved operations as resources are optimized. Part of this journey will likely involve cybersecurity incident response teams deployed across various operational sectors in the economy. These teams will be tasked with detecting, identifying, and containing potential malicious actions. In most cases, the overall process will require support from private sector stakeholders and impact the lives of businesses, communities, and people.

In an ideal world, current defense measures, levels of expertise, systems, and IoT device integration would provide sufficient response capabilities. With today's research, and surveillance systems installed across various countries, we may one day accurately predict when (and where) the next natural disaster may occur. This would allow effective response and mitigation assets to be deployed in advance while allowing critical data to remain secure.

However, the reality is the current COVID-19 pandemic scenario, described as a "gray swan" by risk and resilience practitioners, may occur again in the future. If so, the planning parameters affecting the deployment of public safety and security assets will continue to challenge society. Disruptive critical events often affect every individual while creating opportunities for threat actors. Attackers

exploit times of catastrophe to gain access to critical information on personal mobile devices, or worse, in enterprise critical systems¹³¹.

To illustrate, most buildings and critical infrastructure are managed and supported by building automation systems. These systems regulate airflow, monitor air quality, lighting, water, and electricity, as well as security and fire protection systems. Cyber attacks on building facilities in recent years have been on the rise and can create havoc for occupants of them¹³². Imagine a threat actor gains access to a building's fire protection system. They disable the fire alarms, public broadcast system, and sprinkler pumps during an emergency, resulting in the real loss of lives. The potential level of damage for compromising such systems can be left to one's imagination, especially where national critical infrastructures are concerned.

CRITICAL EVENT MANAGEMENT FOR A SAFE AND SECURE OPERATING ENVIRONMENT

Cyber threats are not confined to digital assets and resources. They can have a physical impact on lives and property. When conventional communication systems are compromised, there is an urgent need to ensure critical communications can continue in a secured and reliable environment. When an unexpected event puts lives at risk, it is crucial to be able to:

- Rapidly notify relevant parties
- Locate and account for missing people and critical resources
- Collect real-time on-the-ground information
- Facilitate the coordination of stakeholders to manage and contain the crisis

The ability to provide an alternative, rapid means of communication is a prudent investment decision. Especially for times when a cybersecurity threat is detected early by the security operations center. Prepared response playbooks can be pre-populated into critical event management platforms. This way, when a significant threat is detected, critical information can be delivered via multiple platforms and integrations (for example, through common platforms such as ServiceNow and Microsoft Teams). Automated response playbooks could also support live operations management and even facilitate forward planning activities.

Current legacy operating systems and devices remain a potential point of entry for threat actors. Businesses or communities that have yet to harness the potential of smart cities are particularly vulnerable. Outdated systems and malicious attackers can greatly hinder attempts to facilitate swift critical event management during a potential crisis. A robust critical event management platform that supports stakeholder collaboration and provides situational awareness can effectively enhance crisis management operations and protect communities and businesses.

THREAT TRENDS TO WATCH IN 2021

BlackBerry researchers and security professionals were asked to provide their cybersecurity predictions for the upcoming year. They ask users to stay aware of the following threat trends as 2021 progresses.



Ransomware Attacks Will Continue to Leverage the Double Extortion Strategy

Threat actors will continue to conduct ransomware attacks while utilizing double extortion to pressure a victim to pay ransom this year. Throughout 2020, cyber criminals strategically stole the victim's data before encrypting it, then threatened to release the stolen information to the public, or even to a competitor. This tactic is used to compel the victim to pay (or at least engage with) the attackers to recover their data. The strategy has driven up the average ransom payments throughout 2020, even though there are no guarantees that attacker-owned copies of the victim's data will be deleted. Instances have been discovered where attackers still released the victim's data even after receiving the ransom payment^{133 134}.



Nation-State Actors Hiding Behind Crimeware-as-a-Service

The emergence, sophistication, and anonymity of crimeware-as-a-service means that nation states can mask their efforts behind third-party contractors and an almost impenetrable wall of plausible deniability. Attackers can obfuscate their efforts to make it appear as though an attack originated almost anywhere. This makes decisively attributing cyber attacks to known threat actors extremely difficult. Companies should consider adapting by applying Zero Trust networking principles and role-based access controls, not just to users, but also to applications and servers.



Threat Actors Contacting Patients as Part of Healthcare Extortion Strategies

Throughout 2020, healthcare organizations continued to top the target list of cyber attacks. The healthcare industry is critical for providing services during the pandemic and also holds confidential data like medical records, which are extremely valuable to attackers. Threat researchers saw cases where medical records were weaponized to facilitate the attacker's objectives.

In October 2020, a Finnish psychotherapy center had their systems attacked and patient data stolen. Not only did the attackers demand a ransom from the psychotherapy center, they also contacted patients individually seeking a ransom of 200 Euros in bitcoin. The threat actors ultimately published the records of at least 300 patients via a Tor site¹³⁵. This tactic could become more popular throughout 2021, especially when combined with traditional ransomware attacks. Furthermore, it could also provide additional pressure on healthcare service providers from patients who are being extorted individually, leading to a higher probability of ransom payment.



Crypto Prices Driving Ransomware Growth

It is generally believed that there is a correlation between the rate of ransomware infections and the price of bitcoin. The value of bitcoin reached all new highs in early 2021¹³⁶. If this assumed correlation holds true, a robust ransomware market can be expected in the near future.

CONCLUSION

The COVID-19 pandemic made a major impact on global systems, and cybersecurity was no exception to its influence. As businesses struggled to survive the disruptive effects of the coronavirus, threat actors moved quickly to capitalize on the resulting chaos. Workers connecting from remote locations, using new devices and untested infrastructure, offered threat actors a rich new attack surface to exploit. People's fear of COVID-19 and understandable desire for information gave attackers new opportunities to launch COVID-19-themed phishing campaigns and malicious apps.

Elections remained vulnerable to cyber attacks through unsecured mobile technology, insufficient DMARC email protection, and over-exposure of personal information on social media. While electronic voting machines are often the center of attention in discussions about election security, it seems attackers favor interfering through more subtle methods. Non-secure political websites, operatives using compromised technology, and over-sharing of personal information on social media all played a role in weakening election security in 2020.

The elusive and highly capable BAHAMUT group remained active in 2020. They trafficked in fake news sites, social media accounts, and hosted dozens of malicious apps in the App Store and Google Play store. BAHAMUT activity currently appears focused in the South Asia and the Persian Gulf regions, though targets in China and Europe have also been discovered. Currently, the group is engaged in credential harvesting from popular sites like Google, Microsoft, Yahoo!, Telegram, Sina, QQ, 126, and 163.

The threat actors behind Emotet continued to refine their attack strategies and capabilities. In 2020, the threat was upgraded to perform Wi-Fi brute force attacks and device infections. It also implemented hash-busting to prevent blacklisting and other security countermeasures. A vulnerability discovered in the malware briefly allowed threat researchers to trigger a kill switch on Emotet infections. The flaw has since been patched.

Ransomware attacks shifted from performing indiscriminate targeting to conducting highly focused campaigns deployed via compromised MSSPs. RaaS is increasingly adopting a private model where affiliates are given access to compromised systems for an agreed cut of future profits. Attackers are favoring exfiltrating data before encryption, then using it to blackmail victims for higher ransoms.

Vehicle manufacturers, facing new regulations, are becoming more cybersecurity conscious. However, connected vehicles remain largely unprotected against a wide range of cyber attacks and data theft. In 2020, the UNECE approved vehicle cybersecurity regulation WP.29 which begins the work of setting common security criterion for global automakers. The first vehicles to benefit from improved security regulations should be on the road by Summer 2024.

The cybersecurity field becomes increasingly complex with each passing year as new technologies, devices, and innovations enter the space. However, the foundation for robust security practices remains unchanged – prepare, prevent, detect, and respond. BlackBerry has delivered secure communications and technology for decades by developing advanced solutions that align with sound security principles. Today, our fifth-generation AI-driven solutions can detect zero-day malware, fileless attacks, insider threats, and more by following the same time-tested security fundamentals.

BlackBerry remains dedicated to advancing the cause of cybersecurity for people and organizations worldwide. We continue to train and deploy increasingly effective and advanced AI models that power our endpoint protection products, with the aim of securing technology, processes, and user identity. We continuously monitor the global threat landscape for emerging threats and seek to provide solutions where problems arise. To learn more about how BlackBerry can secure your technology in 2021 and beyond, visit us at www.blackberry.com [↗](#).

Acknowledgements

The BlackBerry 2021 Threat Report represents the collaborative efforts of our talented teams and individuals. In particular, we would like to recognize:

Alan McCarthy	John de Boer
Anne Kierig	John McClurg
Anuj Soni	John Wood
Baldeep Dogra	Lydia McElligott
Ben Cruz	Marisa Goodrich
Bret Lenmark	Marta Janus
Brian Robison	Natasha Rohner
Claudiu Teodorescu	Nigel Thompson
Dan Ballmer	Sabrina Forgione
Dean Given	Steve Barnes
Ebudo Osime	Thom Ables
Eric Milam	Tim Davies
Gary Ng	T.J. O’Leary
Glenn Wurster	Tom Bonner
Graham Murphy	Tony Lee
Ian Davis	William Savastano
Ieva Rutkovska	Yi Zheng

Legal Disclaimer

The information contained in the BlackBerry Threat Report is intended for educational purposes only. Readers are responsible for exercising their own due diligence when applying this information to their private and professional lives. BlackBerry does not condone any malicious use or misuse of information presented in this report. Trademarks, including but not limited to BLACKBERRY, are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Endnotes

1

<https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/>

2

<https://www.zdnet.com/article/working-from-home-trend-causes-surge-in-cybersecurity-costs-security-breaches/>

3

<https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware>

4

<https://www.fcc.gov/how-identify-and-avoid-package-delivery-scams>

5

<https://cisomag.eccouncil.org/ransomware-attacks-rise-q1-2020/>

6

<https://blogs.blackberry.com/en/2020/05/threat-bulletin-ransomware-2020-state-of-play>

7

<https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report>

8

<https://www.investopedia.com/tech/how-does-bitcoin-mining-work/>

9

<https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html>

10

<https://github.com/xmrig/xmrig>

11

<https://www.darkreading.com/vulnerabilities---threats/cryptojacking-the-unseen-threat/a/d-id/1338903>

12

<https://cointelegraph.com/news/bitcoin-going-parabolic-toward-35k-as-ethereum-breaks-800-what-s-next>

13

<https://www.infosecurity-magazine.com/news/microsoft-warns-of-massive-covid19/>

14

<https://www.geoedge.com/exploit-kits-publisher-protection/>

15

<https://www.zscaler.com/blogs/security-research/top-exploit-kit-activity-roundupspring-2020>

16

<https://threatpost.com/microsoft-exploits-purple-fox-ek/157157/>

17

<https://resources.infosecinstitute.com/topic/purple-fox-malware-what-it-is-how-it-works-how-to-prevent-it/>

18

<https://www.cobaltstrike.com/>

19

<https://www.darkreading.com/threat-intelligence/how-to-identify-cobalt-strike-on-your-network/a/d-id/1339357>

20

<https://www.zdnet.com/google-amp/article/cobalt-strike-and-metasploit-accounted-for-a-quarter-of-all-malware-c-c-servers-in-2020/>

21

<http://www.joeware.net/freetools/tools/adfind/>

22

<https://www.darkreading.com/application-security/ransomware/fin6-expands-its-range-with-ransomware/a/d-id/750703>

23

<https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike>

24

<https://github.com/BloodHoundAD/BloodHound>

25

<https://github.com/BloodHoundAD/SharpHound3>

26

<https://mcpmag.com/articles/2019/11/13/bloodhound-active-directory-domain-admin.aspx>

27

<https://www.zdnet.com/article/malware-gangs-love-open-source-offensive-hacking-tools/>

28

<https://www.andreafortuna.org/2020/09/17/new-mimikatz-update-adds-exploit-for-zeroologon-cve-2020-1472-vulnerability/>

29

<https://stealthbits.com/blog/zeroologon-from-zero-to-hero-part-2/>

30

<https://github.com/AlessandroZ/LaZagne>

31

<https://github.com/skelsec/pypykatz>

32

<https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development>

33

<https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/>

34

<https://www.reuters.com/article/healthcare-coronavirus-astrazeneca-north/exclusive-suspected-north-korean-hackers-targeted-covid-vaccine-maker-astrazeneca-sources-idUSL8N2IC2QU>

35

https://objective-see.com/blog/blog_0x25.html

36

https://objective-see.com/blog/blog_0x51.html

37

<https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/>

38

<https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/>

39

https://objective-see.com/blog/blog_0x59.html

40

https://objective-see.com/blog/blog_0x49.html

41

https://objective-see.com/blog/blog_0x57.html

42

<https://github.com/jgamblin/Mirai-Source-Code>

43

<https://github.com/jgamblin/Mirai-Source-Code/blob/3273043e1ef9c0bb41bd9fcdc5317f7b797a2a94/mirai/bot/scanner.c#L674>

44

<https://whois.arin.net/rest/net/NET-56-0-0-1/pft>

45

<https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>

46

<https://web.archive.org/web/20161022220033/http://hub.dyn.com/dyn-blog/dyn-statement-on-10-21-2016-ddos-attack>

47

<https://threatpost.com/valve-source-engine-fortnite-servers-crippled-by-gafgyt-variant/149719/>

48

<https://malpedia.caad.fkie.fraunhofer.de/details/elf.bashlite>

49

<https://malpedia.caad.fkie.fraunhofer.de/details/elf.tsunami>

50

<https://www.zdnet.com/article/hacker-hundreds-were-tricked-into-installing-linux-mint-backdoor/>

51

<https://threatpost.com/muhstik-botnet-exploits-highly-critical-drupal-bug/131360/>

52

<https://www.anomali.com/blog/the-interplanetary-storm-new-malware-in-wild-using-interplanetary-file-systems-ipfs-p2p-network>

53

<https://www.zdnet.com/article/ipstorm-botnet-expands-from-windows-to-android-mac-and-linux/>

54

<https://www.intezer.com/blog/research/a-storm-is-brewing-ipstorm-now-has-linux-malware/>

55

<https://www.intezer.com/blog/research/a-storm-is-brewing-ipstorm-now-has-linux-malware/>

56

<https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html>

57

<https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf>

58

<https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/>

59

<https://www.cbsnews.com/news/russian-military-officers-hacking-cyber-attacks-charged/>

60

<https://www.justice.gov/opa/press-release/file/1328521/download>

61

<https://www.theguardian.com/us-news/2020/sep/04/us-security-adviser-china-elections-meddling>

62

<https://www.fastcompany.com/90372829/im-a-hacker-and-heres-how-your-social-media-posts-help-me-break-into-your-company>

63

https://dmarc.org/wiki/FAQ#How_does_DMARC_work.2C_briefly.2C_and_in_non-technical_terms.3F

64

<https://www.businesswire.com/news/home/20201022005020/en/Valimail-2020-Election-Infrastructure-Still-Vulnerable-to-Email-Hackers>

65

<https://www.parascript.com/blog/artificial-intelligence-combats-voter-fraud/>

66

<https://www.forbes.com/sites/markminevich/2020/11/02/7-ways-ai-could-solve-all-of-our-election-woes-out-with-the-polls-in-with-the-ai-models/?sh=5511ffcd622c>

67

<https://www.blackberry.com/us/en/forms/enterprise/bahamut-report>

68

<https://attack.mitre.org/software/S0367/>

69

<https://www.silicon.co.uk/security/cyberwar/banking-trojan-emetet-returns-220593?cmpredirect>

70

<https://thehackernews.com/2020/11/anyrun-emetet-malware-analysis.html>

71

<https://cyware.com/news/the-evolution-of-the-infamous-emetet-banking-trojan-28f517ac/>

72

<https://www.bankinfosecurity.com/emetet-malware-returns-to-work-after-holiday-break-a-11955>

73

<https://blog.barracuda.com/2020/06/19/emetet-emerges-as-a-leader-in-maas/>

74

https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/2019/BBCylance_LC_Q319_Threat_Report.pdf

75

<https://us-cert.cisa.gov/ncas/alerts/TA18-201A>

76

<https://www.cybereason.com/blog/one-two-punch-emetet-trickbot-and-ryuk-steal-then-ransom-data>

77

<https://www.zdnet.com/article/banking-malware-finds-new-life-spreading-data-stealing-trojan/>

78

<https://www.zdnet.com/article/malware-and-botnets-why-emetet-is-dominating-the-malicious-threat-landscape-in-2019/>

79

<https://resources.infosecinstitute.com/topic/emetet-returns-with-new-improvements/>

80

<https://threatpost.com/emetet-now-hacks-nearby-wi-fi-networks-to-spread-like-a-worm/152725/>

81

<https://thehackernews.com/2020/08/emetet-botnet-malware.html>

82

<https://iotnowtransport.com/2019/04/09/71897-automotive-industry-struggles-navigate-cybersecurity-issues/>

83

<https://dzone.com/articles/study-shows-security-challenges-in-the-auto-indust>

84

<https://blog.guardknox.com/what-are-connected-vehicles-and-their-vulnerabilities>

85

<https://www.strategyanalytics.com/strategy-analytics/blogs/automotive/infotainment-telematics/infotainment-telematics/2018/11/27/auto-cyber-security-from-ignore-to-compliance>

86

<https://www.ic3.gov/Media/Y2016/PSA160317>

87

<https://www.ibtimes.com/tesla-model-s-hack-oslo-based-security-firm-uses-android-hack-unlock-steal-car-2450833>

88

<https://www.sciencedirect.com/science/article/pii/S221420961930261X>

89

<https://www.wmctionnews5.com/story/39022826/used-cars-increase-identity-theft-chances-bbb-finds/>

90

<https://www.edmunds.com/car-technology/car-technology-and-privacy.html>

91

<https://arstechnica.com/information-technology/2019/10/five-months-after-returning-rental-car-man-still-has-remote-control/>

92

<https://www.theguardian.com/technology/2020/feb/18/smart-car-gig-rental-app-trapped>

93

<https://argus-sec.com/unece-wp29-approved/>

94

<https://unece.org/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-1073r27e.pdf>

95

<https://unece.org/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll-out-connected-vehicles>

96

<https://www2.deloitte.com/global/en/blog/responsible-business-blog/2020/new-cybersecurity-regulations-challenge-automobile-manufacturers.html>

97

<https://blogs.blackberry.com/en/2020/05/threat-bulletin-ransomware-2020-state-of-play>

98

https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

99

<https://apwg.org/trendsreports/>

100

<https://www.microsoft.com/security/blog/2020/07/08/protecting-remote-workforce-application-attacks-consent-phishing/>

101

<https://info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset>

102

<https://cofense.com/mfa-bypass-phish-caught-oauth2-grants-access-user-data-without-password/>

103

<https://www.proofpoint.com/us/blog/threat-insight/ta2552-uses-oauth-access-token-phishing-exploit-read-only-risks>

104

<https://www.bbc.com/news/technology-48908736>

105

<https://www.forbes.com/sites/daveywinder/2019/10/08/forget-2020-election-fake-news-deepfake-videos-are-all-about-the-porn/?sh=42537b4b63f9>

106

https://cpb-us-e1.wpmucdn.com/sites.uw.edu/dist/6/4560/files/2020/10/CIP_Deepfakes_Report_Extended.pdf

107

<https://www.brusselstimes.com/news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/>

108

<https://www.nbcnews.com/tech/tech-news/russian-internet-trolls-hired-u-s-journalists-push-their-news-n1239000>

109

In December 2020 a “highly sophisticated nation-state actor” (according to the Cybersecurity and Infrastructure Security Agency (CISA)) compromised certain SolarWinds software widely used across private/public to monitor health of cyber networks. CISA had to issue an emergency cybersecurity directive ordering all federal agencies to disconnect or power-down certain SolarWind products.

110

<https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216>

111

<https://priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/>

112

<https://priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/>

113

<https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading?source=email>

114

<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>

115

<https://www.publicsafety.gc.ca/cnt/rsrcls/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf>

116

<https://www.issa.org/the-impact-of-the-covid-19-pandemic-on-cybersecurity/>

117

<https://us-cert.cisa.gov/ncas/alerts/aa20-099a>

118

<https://www.mirror.co.uk/tech/android-warning-fake-coronavirus-safety-21759866>

119

<https://www.cnet.com/health/fbi-issues-warning-for-covid-19-stimulus-package-scams/>

120

<https://www.seattletimes.com/seattle-news/state-auditor-weak-security-accounting-errors-in-600-million-unemployment-fraud/>

121

<https://www.cnet.com/news/hurricane-harvey-charity-donations-scam-phishing-attack/>

122

<https://www.cnet.com/news/man-charged-in-katrina-web-scam/>

123

<https://threatpost.com/working-from-home-covid-19s-constellation-of-security-challenges/153720/>

124

<https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/>

125

<https://www.who.int/about/communications/cyber-security>

126

<https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast>

127

<https://www.cnet.com/news/vpn-use-surges-during-the-coronavirus-lockdown-but-so-do-security-risks/>

128

<https://vpnpro.com/blog/google-removes-one-of-biggest-vpn-apps-from-play-store-due-to-vulnerability/>

129

<https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html>

130

<https://www.blackberry.com/us/en/solutions/zero-trust>

131

INTERPOL – Global Landscape on COVID-19 Cyber Threat (April 2020)

132

<https://www.facilitiesnet.com/buildingautomation/tip/Smart-Buildings-At-High-Risk-for-Cyber-Attacks-Study--44839>

133

<https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

134

<https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/>

135

<https://apnews.com/article/psychotherapy-cabinets-finland-6b27c895df0abd532a4fb000c9d5d517>

136

<https://www.cnn.com/2021/01/07/bitcoin-btc-rally-extends-price-hits-record-high-above-37700.html>

