Everything You Need to Know About Callback Phishing

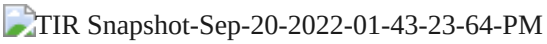
Archived: 2026-11-28 02:17:25 UTC

Executive Summary

In October 2021, Avertium's Cyber Threat Intelligence Team published a Threat Intelligence Report regarding the healthcare industry and why the industry is constantly at risk for security incidents. The industry is two to three times more likely to be a target for cybercrime than any other industry. One of the ways the industry is currently being attacked is via callback phishing – an attack vector used by Quantum and Ryuk ransomware gangs.

During the second quarter of the year, Agari published a cyber threat intelligence report regarding phishing attacks. The report stated that although phishing volumes have increased by 6% compared to the first quarter of the year, hybrid vishing has seen massive growth at 625%. This indicates that threat actors are moving away from relying solely on traditional phishing to breach networks and are moving toward a hybrid approach.

Threat actors such as Quantum and Ryuk have used callback phishing to impersonate countless companies. Let's take a look at callback phishing, the threat actors who use the attack vector, and why organizations everywhere need to be on high alert.


TIR Snapshot-Sep-20-2022-01-43-23-64-PM

what is callback phishing?

Callback phishing is a type of phishing attack that impersonates a business. The attack starts off as a phishing email, typically claiming that the victim needs to renew a subscription or pay a bill for a service that they did not purchase. The email contains a "customer service" phone number with direction to call if the victim has questions and concerns.

What the victim does not know is that the email is a phishing email and once they dial the customer service number, there is a threat actor who picks up. The attacker then attempts to collect confidential information to validate the "transaction". The information collected is sensitive and primarily includes credit card and bank account information. After the attacker gets the information they need, the call ends, and the victim's accounts are compromised.

What makes this attack unique is that callback phishing emails can bypass email filters because they don't include malicious links or attachments with malware. Instead, the phishing attacks are heavily focused on social engineering. This means that because email filters generally won't catch the phishing attempt, it is up to the user to be able to spot the warning signs.

callback phishing attacks

In June 2022, the Conti ransomware gang shut down their operations. However, this was not the end of Conti, and it was confirmed by Avertium's technology partner, AdvIntel, that in August 2022 the gang splintered into smaller

groups on their own. At least three of those groups (Quantum, Silent Ransom, and Roy/Zeon) have been observed using BazarCall, also known as callback phishing. According to AdvIntel, when Conti dissolved, members of the group decided to distance themselves from the toxic Conti brand. The two largest divisions of Conti created their own collectives – Team Two created the current version of Quantum, while Team One created Roy/Zeon.

The attack vector allowed the original Conti to deploy highly targeted attacks that were difficult to detect due to the social engineering aspect of the attack. In 2021, the Ryuk ransomware gang also used callback phishing in their ransomware operation. Ryuk was later rebranded into Conti; therefore, it makes sense that other groups associated with the threat actor are using callback phishing now.

The Ryuk ransomware gang was known for exploiting two vulnerabilities to increase their permissions on compromised machines:

- **CVE-2018-8453** – a privilege escalation vulnerability affecting Windows 7 through Windows 10, as well as Windows Server 2008 through 2016. The vulnerability allowed attackers to run an arbitrary kernel with read/write permissions due to the Win32k component failing to properly handle object in memory.
- **CVE-2019-1069** – a privilege escalation vulnerability affecting Windows Server 2016 and 2019, as well as Windows 10. The vulnerability allowed a hard link attack due to the way the Task Scheduler Service validated certain file operations.

Ryuk was a veteran ransomware gang that had been in the ransomware business for several years. They were estimated to have collected at least $150 million in ransom payments – one victim paying $34 million to restore their system. Ryuk ransomware has been used by a group called “Wizard Spider”. This group uses several other tools, including a tool called Trickbot. We were unable to find a Ryuk sample; however, Avertium’s Cyber Threat Intelligence team (CTI) was able to find a Trickbot sample.

Image 1: Ryuk - Trickbot Sample



Source: Avertium's Cyber Threat Intelligence Team

If we decompile this binary, we find a few more API calls and functions that might indicate functionality. There are functions for creating a timer and deleting a timer, which can also be used to evade detection or frustrate malware analyst.

Image 2: Ryuk Function Calls



Source: Avertium's Cyber Threat Intelligence Team

As previously stated, Avertium published a Threat Intelligence Report featuring Quantum ransomware and their use of BazarCall, which they were calling Jormungandr (which means Midgard Serpent or World Serpent in Norse Mythology). Quantum’s Jormungandr campaign is a major development that Quantum has been preparing for since June 2022. The phishing campaign is a derivative of BazarCall, and initial access is achieved by utilizing IcedID for reconnaissance tasks, as well as persistence. The DFIR Report published a case summary in April 2022

that showed the threat actors entering a victim's network when a user endpoint was compromised by an IcedID payload contained within an ISO image, likely delivered via email.

AdvIntel confirmed that Quantum was the main Conti subdivision (Team Two) and was responsible for breaching the Costa Rica government – a feat they accomplished before they "shut down". If you recall, Costa Rica had to issue a state of emergency as a result of Conti's attack. When Quantum initially emerged in September 2021, they were actually a rebrand of MountLocker – a group that was responsible for attacking biotech companies.

In order for Quantum's callback phishing to be a success, they impersonate well-known brands. Those brands included Gobble, Oracle, HelloFresh, Luchechko Mortgage Team, the US Equal Opportunity Employment Commission, and Crowdstrike. When they impersonated these brands, they first sent an email encouraging recipients to call a number for further clarification.

CrowdStrike, a well-known cybersecurity company, was impersonated by Quantum in July 2022 when the attackers sent a professional email targeting the company's employees. The email stated that a network compromise was identified during their routine audit, and they needed to call a number to discuss the situation and provide additional information. Again, the email didn't contain any malicious links, making it unlikely to be flagged by anti-phishing security solutions.

The attackers used social engineering to guide the employees into installing remote administration tools (RATs) that allowed the Quantum to take control over their workstations. From there, the threat actors were able to remotely install additional tools that allowed them to move laterally through the network, deploy more ransomware, and steal data. As a result of Quantum's attack, Crowdstrike had to notify the public and stated that the attack would likely lead to a ransomware attack. At the time, it was the first identified callback campaign that impersonated a cybersecurity company.

Crowdstrike stated in their notice to customers that the company identified a similar callback campaign in March 2022 where threat actors installed AteraRMM followed by Cobalt Strike to assist with lateral movement and to deploy additional malware.

Avertium's CTI team analyzed a Quantum ransomware sample. The team was only able to find one sample related to Quantum ransomware and the sample contained only the dll. This is one of many factors that make this malware a bit harder to analyze. Without more context regarding the execution of the binary, it becomes much more difficult to replicate the conditions in which this program was designed to execute.

The typical methods of execution did not result in successful encryption of the CTI team's test machine. This could be due to additional functionality built into the program to fail if it detects it in a virtual environment.

Despite these difficulties, we can still glean some interesting information through static analysis. We can confirm that this is an executable Windows DLL, and was compiled in late November of 2021.

Image 3: Quantum File Type Analysis

Quantum File Type Analysis

Source: Avertium's Cyber Threat Intelligence Team

Image 4: Quantum Executable Header Information


Quantum Executable Header Information

Source: Avertium's Cyber Threat Intelligence Team

We can also see some of the API calls that this program makes, which gives at least some indication of its functionality. For instance, it calls “LoadLibraryA”. This is used to load a specified module into the address space of the calling process and can be used by the malware to avoid detection or for injection into a different process.

Image 5: Quantum API Calls


Quantum API Calls

Source: Avertium's Cyber Threat Intelligence Team

Prevention

Because traditional anti-phishing software does not detect callback phishing emails, it is important for organizations to train their staff on how to spot one. As stated previously, callback phishing attempts start off as an email and will encourage the target to call a number to speak with a customer service representative about a subscription or bill. Here are a few ways you can help keep your organization safe and secure from callback phishing attempts:

- **Review –** Organizations and individuals should ensure that they know when there is a legitimate company trying to reach them. One can do this by clicking on the email sender’s email address and verifying if the sender is from the expected organization’s domain. If there are any misspellings or suspicious characters in an email address, then the sender is likely trying to spoof a company.

For example, if Avertium’s typical customer service emails always come from this email address “Avertium.Customer.Service.com” and all of a sudden you receive a customer service email from “Avertim_Customer.Service.com” with the Avertium logo and a callback number for customer service, it is likely to be a callback phishing attempt.

- **Ask yourself some questions –** If language in an email keeps trying to convince you to do something with urgency, that is a red flag. Cybercriminals are always very persistent in their phishing emails and just like traditional phishing emails, they will try to be convincing in getting you to call a phone number.

Be diligent in verifying telephone numbers before calling, just as you would for traditional phishing emails with suspicious links. Always look up contact numbers from the organization’s official website.

- **Ask for help –** If you follow the above steps and are still skeptical about the email, reach out to someone for help. Your IT team will more than likely help you and do further digging. A false alarm is better than setting off a real one.

How Avertium is Protecting Our CUSTOMERS

It's important to get ahead of the curve by being proactive with protecting your organization, instead of waiting to put out a massive fire. Avertium offers the following services to keep your organization safe:

- Expanding endpoints, cloud computing environments, and accelerated digital transformation have decimated the perimeter in an ever-expanding attack surface. Avertium's offers Attack Surface Management, so you'll have no more blind spots, weak links, or fire drills.
- Fusion MXDR is the first MDR offering that fuses together all aspects of security operations into a living, breathing, threat-resistant XDR solution. By fusing insights from threat intelligence, security assessments, and vulnerability management into our MDR approach, Fusion MXDR offers a more informed, robust, and cost-effective approach to cybersecurity – one that is great than the sum of its parts.
- Avertium offers VMaaS to provide a deeper understanding and control over organizational information security risks. If your enterprise is facing challenges with the scope, resources, or skills required to implement a vulnerability management program with your team, outsourced solutions can help you bridge the gap.
- Avertium offers Zero Trust Architecture, like AppGate, to stop malware lateral movement.
- Avertium offers user awareness training through KnowBe4. The service also Incident Response Table-Top exercises (IR TTX) and Core Security Document development, as well as a comprehensive new-school approach that integrates baseline testing using mock attacks.

Avertium's Recommendations

- Quantum utilizes data encryption as a part of its ransomware locker. Organizations should implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and severs in a separate, segmented, and secure location.
- Organizations should implement network segmentation and have offline backups of data.
- Back up data regularly and password protect backup copies offline. Copies of critical data should not be accessible for modification or deletion from the system where data resides.
- Organizations should emphasize network investigation tools that are used for exfiltration-centric groups (Cobalt Strike, Metasploit, and customized PowerShell Commands.
- Track abnormal signaling to assist in identifying beacons.
- The BazarCall attack vector relies on the execution of a beacon or malicious payload into the network system, which is liable to spread to other devices on the network. Separating the device while mitigating the BazarCall breach minimizes the chance that the infection will be able to affect other devices.
- To identify Cobalt Strike, examine the network traffic using TLS inspection, then isolate bot traffic and identify the suspicious traffic by examining data within HTTPS requests.
- **Network Based Security Practices**
    - Use and maintain anti-virus software and a firewall.
    - Regularly scan for spyware.
    - Keep software up to date.
    - Evaluate your software settings.
    - Avoid unused software programs.
    - Establish guidelines for computer use.
    - Encrypt sensitive files.

- Dispose of sensitive information properly.

MITRE Map

Quantum


Quantum MITRE Map

Indicators of Compromise (IoCs)

Quantum

Files

- docs_invoice_173[.iso]
- e051009b12b37c7ee16e810c135f1fef
- 415b27cd03d3d701a202924c26d25410ea0974d7
- 5bc00ad792d4ddac7d8568f98a717caff9d5ef389ed355a15b892cc10ab2887b
- Dar[.dll]
- 4a6ceabb2ce1b486398c254a5503b792
- 08a1c43bd1c63bbea864133d2923755aa2f74440
- 4a76a28498b7f391cdc2be73124b4225497232540247ca3662abd9ab2210be36
- Document[.lnk]
- adf0907a6114c2b55349c08251efdf50
- aa25ae2f9dbe514169f4526ef4a61c1feeb1386a
- 3bb2f8c2d2d1c8da2a2051bd9621099689c5cd0a6b12aa8cb5739759e843e5e6
- Adf[.bat]
- ebf6f4683d8392add3ef32de1edf29c4
- 444c704afe4ee33d335bbdfae79b58aba077d10d
- 2c2513e17a23676495f793584d7165900130ed4e8cccf72d9d20078e27770e04
- Ulfefi32[.dll]
- 49513b3b8809312d34bb09bd9ea3eb46
- 445294080bf3f58e9aaa3c9bcf1f346bc9b1eccb
- 6f6f71fa3a83da86d2aba79c92664d335acb9d581646fa6e30c35e76cf61cbb7
- License[.dat]
- e9ad8fae2dd8f9d12e709af20d9aefad
- db7d1545c3c7e60235700af672c1d20175b380cd
- 84f016ece77ddd7d611ffc0cbb2ce24184aeee3a2fdbb9d44d0837bc533ba238
- Ttsel[.exe]
- b1eff4fffe66753e5f4265bc5332f72e
- da2caf36b52d81a0d983407ab143bef8df119b8d
- b6c11d4a4af4ad4919b1063184ee4fe86a5b4b2b50b53b4e9b9cc282a185afda

- p227[.dll]
- 350f82de99b8696fea6e189fcd4ca454
- deea45010006c8bde12a800d73475a5824ca2e6f
- c140ae0ae0d71c2ebaf956c92595560e8883a99a3f347dfab2a886a8fb00d4d3

IcedID

- dilimoretast[.]com
- antnosience[.]com
- oceriesfornot[.]top
- 138[.]68.42.130:443
- 157[.]245.142.66:443
- 188[.]166.154.118:80

Cobalt Strike

- C2/IP: 185.203.118[.]227:443
- Watermark: 305419776

Network Detections

- ET MALWARE Observed Malicious SSL Cert (Fake Gmail Self Signed - Possible Cobalt Stirke)
- ET POLICY SMB2 NT Create AndX Request For an Executable File In a Temp Directory
- ET MALWARE Win32/IcedID Request Cookie
- ET POLICY PE EXE or DLL Windows file download HTTP
- ET POLICY PsExec service created
- ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
- ET POLICY SMB2 NT Create AndX Request For an Executable File
- ET DNS Query to a *.top domain - Likely Hostile
- ET INFO HTTP Request to a *.top domain
- ET POLICY SMB Executable File Transfer

BazarBackdoor, Conti, TrickBot

Hashes

- 078d12bdc207572f9972d393790ea90d
- 5e61a7988375efe18897ff264b7c81b8
- f4dc5b1151ed77bfcfae8b73147d93c2
- 8a487c189edd6e3cc32cee7709aa4e0c21d07491
- e0aef96555318bac394065c9721c0310ca0df091
- e53166ca0f09ad46795cd8f5a1c9a4a2d5b21415
- 71cd6cb93fcf508761b72fac05bc96a07697718eb928c72fc7731dab457b3606
- 7aa4cb052ddfbccac10bdfeae585f15fa4bfbeadea5ece649234fcbc9fec2955
- a9d8ae5ac1ac15a440d8d5e61287eb352f9da7cca60ce88727d338e960d8d461
- 01bda7c837d67a41eb0fbe0b79e6042d

- 01d3e51b4af8d3d9f662c23ece654f5d
- 097cb948a1f011f5de11579849a08db5
- 0a660a846d152eec379718d9e16fbf7f
- 0e7f9df69d9765981bce46bc376811a5
- 120cf4d1f8e624642afa69869ae1af6b
- 12963009969137f99d02129f98465975
- 1737388ce8b0b5fc2dbc22f5b7352b7c
- 1a0dfbd78d21316167f4a05f56e25e6f
- 1cb1a805d778e782a8fc0614d83970c0
- 1f46d93baf23dec9d0073c807f1d3c5e
- 21807bf30699429100f07c674e9f52f0
- 21e3cae5b77c41528658ada08509c392
- 2237dd795e50a6d4ef1bd3bafa8c771f
- 256fa0ae50b4e199b631047f2fe98b58
- 27b341fa2aa731335273204cb112a414
- 2b14db199e034461e2302c90d61b0e1a
- 2c00aaba1bad8a20cf1f154646e50878
- 2c4ba65ebe45a97b6e43a971c6ad580b
- 2d72690d5ddb20e33d0c7a1a6a4e7077
- 309368b122ab63103dddd4ad6321a82c
- 31ca2341e48b6f67b02cebdeac30b321
- 4167a72b3e4e42cfe486885b7795bdf5
- 441a9b57a778665b0689986265a59caf
- 47f3d75c9d69600d32078f532318e688
- 48ca84fcc3a4d8bffbd48b12b4e1d4b1
- 494e8dc63210ed59ab012ebb5be1a283
- 4cc5e4698356389551644 95e1069b54a
- 4d373fda8175a8c79e2e0dc760325634
- 4d8af5ba95aa23f7162b7bbf8622d801
- 52fd3e86aad283c1958c2babbba5d0bc
- 553a3cbe0b19e58c5d48e9b0396690bf
- 5628e7821300674c1d2d197c36ae27de
- 56c552097559ecbafedd5683038ca480
- 57d2519d7d59a34d9b7b51702b202993
- 587a9cbcaec3ddceeba5a0fadd601d2d
- 5c1fce8fa3e228b8f2641bb1f7a29c3f
- 5da1ec0c2839285fd6e098e3ffd5874b
- 6349d5381beae42063ede8cb76143267
- 6798ff540f3d077c3cda2f5a4a8559f7
- 69c68c62844966115c13dfee2e7bc58c
- For additional IoCs, click here.

Supporting Documentation

[10 key facts about callback phishing attacks - CyberTalk 2022]

[Callback phishing attacks see massive 625% growth since Q1 2021 (bleepingcomputer.com)]

[Uptick in Callback Phishing Attacks is a Timely Cyber Security Reminder (deandorton.com)]

[Ransomware gangs move to 'callback' social engineering attacks (bleepingcomputer.com)]

[Cybereason vs. Quantum Locker Ransomware]

[An In-Depth Look at Quantum Ransomware (avertium.com)]

[Hackers impersonate cybersecurity firms in callback phishing attacks (bleepingcomputer.com)]

[Callback Phishing Campaigns Impersonate CrowdStrike, Other Cybersecurity Companies]

[CrowdStrike Warns About Callback Phishing Attacks Impersonating Cybersecurity Companies - CPO Magazine]

[Uptick in Callback Phishing Attacks is a Timely Cyber Security Reminder (deandorton.com)]

[Ryuk ransomware operation updates hacking techniques (bleepingcomputer.com)]

[Ryuk Ransomware's Increased Activity Targets Large Organizations Using Windows OS (avertium.com)]

[Ryuk Ransomware Common Activities and IOCs | Proficio Threat Intel]

[IOCs for BazarBackdoor, Conti, Diavol, Ryuk, TrickBot, WizardSpider 05042022 - AlienVault - Open Threat Exchange]

APPENDIX II: Disclaimer

This document and its contents do not constitute, and are not a substitute for, legal advice. The outcome of a Security Risk Assessment should be utilized to ensure that diligent measures are taken to lower the risk of potential weaknesses be exploited to compromise data.

Although the Services and this report may provide data that Client can use in its compliance efforts, Client (not Avertium) is ultimately responsible for assessing and meeting Client's own compliance responsibilities. This report does not constitute a guarantee or assurance of Client's compliance with any law, regulation or standard.

COPYRIGHT: Copyright © Avertium, LLC and/or Avertium Tennessee, Inc. | All rights reserved.

Related Resource: [4 Trending Phishing Techniques and Tips for Detection]

Chat With One of Our Experts

Source: https://web.archive.org/web/20251104184302if_/https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-callback-phishing