ZeroFOX Quarterly Threat Landscape Review

Q1 2021

ZEROFOX

Table of Contents

Executive Summary

In the first quarter (Q1) of 2021, the global cyber threat landscape exhibited a series of events that included takedowns of criminal infrastructure, the persistence of ransomware extortion schemes, and creative tools and techniques used to deliver malicious artifacts to victims. Law enforcement agencies worldwide worked together to disrupt criminal operations in credit card networks, ransomware groups, and botnet infrastructure. The success of ransomware double extortion tactics led to the continuation of this method as new ransomware types emerged and operators used grey hat tactics to justify their criminal actions. Threat actors leveraged creative delivery tools and techniques that evade detection by security technologies and make analyzing cyber threats more complex. In underground cyber communities, ZeroFOX Research observed significant competition among threat actors due to increased traffic in marketplace networks. The investigation of the December 2020 SolarWinds Orion breach continued in Q1, with security researchers identifying six malware types used in the breach. Another large-scale attack took place against Microsoft Exchange Servers this quarter in which threat actors exploited a set of vulnerabilities to access target environments and install malware. Furthermore, four key industries faced cybersecurity risks due to COVID-19-themed threats, vulnerable infrastructure, and evolved technology. In this Quarterly Threat Landscape Review, ZeroFOX Research provides an overview and analysis of the prominent threats in Q1 2021.

Key Points

- The takedown efforts aimed at criminal operations were the direct result of international law enforcement officials working together to mitigate hostile threats impacting businesses and individuals.

- Ransomware double extortion schemes persisted in 2021 as ransomware operators introduced new types of ransomware, updated existing ransomware, and used "grey hat" tactics to justify criminal operations.

- Threat actors used creative tools and techniques to distribute threats that involved Morse code to evasively spread phishing URLs and continued use of remote desktop protocol (RDP) exploits to target individuals working from home.

- The increased activity in cyber underground marketplaces contributed to competition among threat actors, resulting in manipulation, misinformation, and exposure of threat actor aliases.

- Security researchers identified six malware types in the SolarWinds Orion breach used by unaffiliated threat actors groups based in Russia and China.

- New vulnerabilities and exploits disclosed this quarter included security flaws pertaining to a large-scale attack on the Microsoft Exchange mail server that allowed attackers to execute remote commands, install malware, and steal data from the target environment.

- Underground marketplaces and chat networks exhibited instances of threat actors continuing to take advantage of COVID-19-themed lures, from fraudulent pandemic assistance schemes to vaccine distribution scams.

- The incident involving the poisoning of a Florida water system underscored the need for industrial control systems organizations to have sufficient resources directed towards updating older networks to be securely operated.

- Increased online sales heightened the need for retailers to rethink e-commerce security, as threat actors use digital skimming technologies to carry out malware attacks and data leaks on e-commerce platforms.

Criminal Operation Takedowns

As more cyber threats emerge on the threat landscape, security researchers must tackle sophisticated, targeted, and aggressive threats. The rate and impact of such threats make it critical for security experts and law enforcement to take action to mitigate potential cyber attacks. Towards the end of 2020 and into Q1 of 2021, law enforcement agencies worldwide worked together to disrupt high-profile criminal operations, which led to the arrest of threat actors and the confiscation of malicious artifacts. Three well-known criminal operations were affected by the disruption effort: Joker's Stash carding forum, Egregor ransomware, and Emotet botnet. The chart seen in Figure 1 details this takedown activity.

Name	Type	Take Down Details
Joker's Stash	Carding forum	Joker's Stash announced they were suspending operations in January 2021. The announcement came after a turbulent 2020 during which law enforcement shut down four domains operated by the Joker's Stash team.
Egregor	Ransomware	In February 2021, French and Ukrainian law enforcement officials arrested Egregor operators in Ukraine.
Emotet	Botnet	North American and European law enforcement (with assistance from Europol) collaborated to disrupt Emotet by taking control of the infrastructure from inside the botnet.[1]

Figure 1: Prominent takedown activity in Q1 2021
Source: ZeroFOX Research

The demand for law enforcement to take action on cyber criminal operations comes after threat actors caused businesses significant financial and operational damage. Carding forums like Joker's Stash account for millions of records containing compromised financial credentials. Threat actors use these marketplaces to upload information from data leaks to sell to other threat actors. In 2020, Joker's Stash posted over 35 million records of card present data and over eight million records of card-not-present data.[2] (**ZeroFOX Note**: *Card present* refers to credit card transactions where the cardholder is present during the transaction. *Card-not-present* refers to transactions where the cardholder or credit card is not present during the transaction.[3])

Unlike carding marketplaces, ransomware and botnet malware can have lasting effects on businesses—primarily by the way of lengthy recovery times, costly investigations, and a possible pause on daily operations. Egregor ransomware's success resulted from combining skilled attackers previously affiliated with earlier ransomware operations and double extortion

schemes. The skills and expertise of Egregor operators made the ransomware a high-risk threat to both large and small organizations, which ultimately resulted in over 200 victims being exposed on the group's data leak website.[4]

The Emotet botnet was used by other malware, like Trickbot, to conduct spamming activity and infect target machines. Emotet has gone through various updates and iterations since it first emerged on the threat landscape in 2014 as a banking trojan. The botnet was particularly damaging, as Emotet's operators relied heavily on evasion to ensure successful attacks. This fact, combined with its partnership with Trickbot threat actors, made Emotet a high-level threat that required organizations to be vigilant about Emotet-delivered phishing attacks.

While the disruption effort by law enforcement is intended to permanently terminate cyber criminal operations, threat actors manage to develop new resources that allow them to engage in cyber crime and nefarious activity. Cyber underground communities contain numerous carding networks, and threat actors that once used Joker's Stash's services will shift to another service that offers more options and features. In terms of malware, as-a-service frameworks are bought and sold on underground marketplaces that allow threat actors to customize malware that rivals Egregor and Emotet. Dutch authorities conducted a mass uninstall of Emotet from infected devices on March 25, 2021, and are confident that Emotet will not reemerge, as they seized all Emotet infrastructure to prevent threat actors from reviving it. Towards the end of 2020, a joint effort between U.S. Cyber Command and Microsoft was undertaken to disrupt the Trickbot malware. However, Trickbot was restored to its former state, and operators launched an updated version of Trickbot in Q1 2021 that incorporated "Massscan," a tool that scans local networks for other systems with open ports to attack at a later stage.[5] Trickbot's activity within the past quarter underscores the resiliency of some malware, even after facing the threat of termination. Nevertheless, only time will tell if the disruption efforts by authorities will have lasting effects.

Ransomware

Double Extortion Schemes

Double extortion schemes occur when ransomware teams threaten to leak their victims' stolen information if ransom demands go unpaid; the team ransoms the encrypted files *and* the data obtained during the infection. These tactics became successful in 2020 due to victims' fear of having their sensitive information publicly exposed and potentially sold to threat actors and have continued to flourish in 2021. Q1 2021 metrics revealed that Conti ransomware was responsible for nearly 23 percent of known double extortion activity over the quarter, followed by Avaddon, Sodinokibi/REvil, and DoppelPaymer ransomware. Figure 2 displays a chart of the overall volume of double extortion victims categorized by ransomware groups.

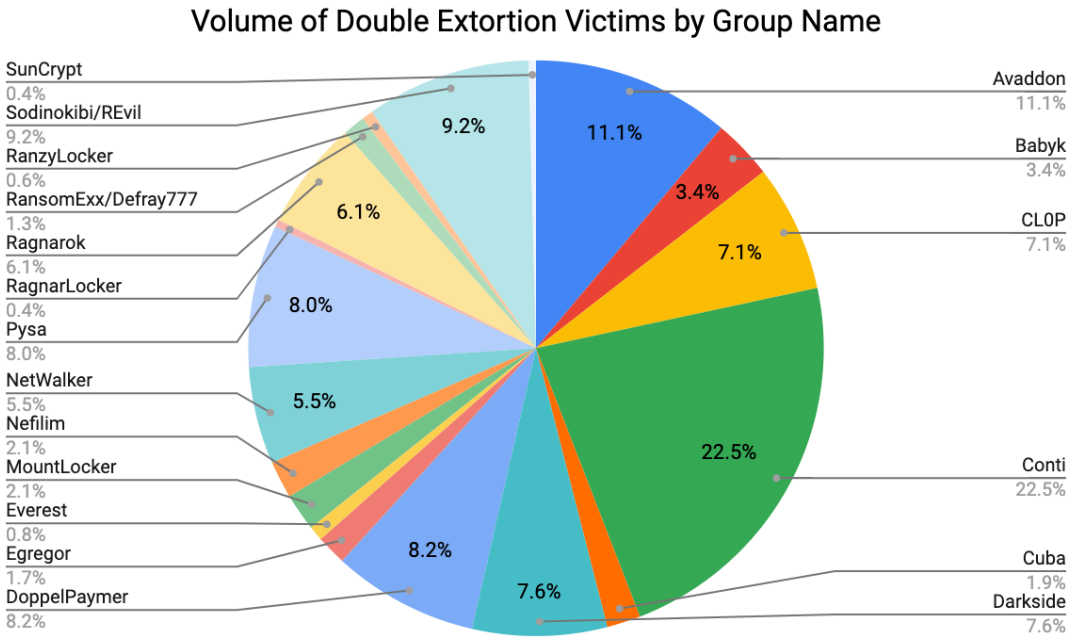


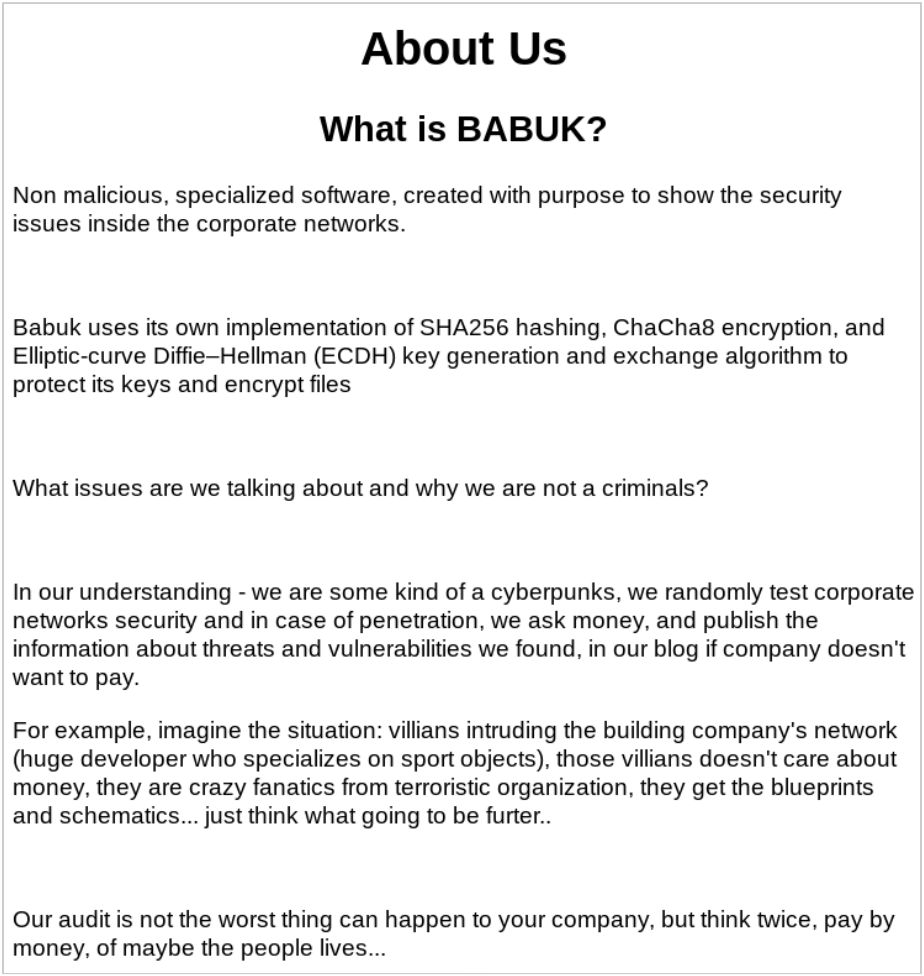
Figure 2: Overall volume of double extortion victims by group
Source: ZeroFOX Research

Grey Hat Operations

Another trend among ransomware groups is justifying nefarious activity by claiming the attack is a grey hat operation. The term "grey hat" refers to security researchers who violate computer laws or ethical standards but without malicious intent. In terms of ransomware, some ransomware operators state that the purpose of their activity is to expose victims that lack robust security and infrastructure. One of the first grey hat claims was in November 2020, when Maze ransomware terminated their operations and posited that they exposed victims that

lacked adequate data storage security, specifically when protecting clients' sensitive information.[6]

In Q1 2021, other ransomware groups also demonstrated approaches aimed at exposing organizations with weak security. For instance, the Babyk (also known as Babuk Locker) ransomware operators indicated to victims that their ransomware was not malicious but was instead a way for victims to learn about their systems' flaws. Babyk further asserts that they label themselves as "cyberpunks'' versus threat actors because they use penetration testing to assess the security of corporate networks and subsequently publish the information they find only if companies do not compensate them for their discoveries. Figure 3 is a screenshot of the Babyk ransomware's "About Us'' page (hosted on their data leak website) containing details about the group and their operations.



About Us

What is BABUK?

Non malicious, specialized software, created with purpose to show the security issues inside the corporate networks.

Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to protect its keys and encrypt files

What issues are we talking about and why we are not a criminals?

In our understanding - we are some kind of a cyberpunks, we randomly test corporate networks security and in case of penetration, we ask money, and publish the information about threats and vulnerabilities we found, in our blog if company doesn't want to pay.

For example, imagine the situation: villians intruding the building company's network (huge developer who specializes on sport objects), those villians doesn't care about money, they are crazy fanatics from terroristic organization, they get the blueprints and schematics... just think what going to be furter..

Our audit is not the worst thing can happen to your company, but think twice, pay by money, of maybe the people lives...

Figure 3: Babyk ransomware's "About Us" page
Source: ZeroFOX Research

In February 2021, security researchers published an article interviewing one of the operators behind the LockBit ransomware. The interview shed light on current ransomware operations and why some threat actors choose to work with ransomware. According to researchers, the operator is likely based in Russia and has been working with ransomware for several years.[7] Cyber crime became appealing to the actor because they could make more money than in their conventional IT career, allowing them to better provide for their family. The actor discussed that they targeted victims based on who would choose to pay ransom demands quickly. The operators used new exploits to infect victims because companies were less likely to patch the flawed software. Furthermore, the actor informed victims of the consequences of not properly securing data and received compensation for identifying threats. This last point demonstrates that using grey hat tactics provided LockBit operators a way in which to justify criminal actions.

Creative Delivery Tools and Techniques

In Q1 2021, threat actors used both new and creative delivery techniques to spread threats to intended targets. A new technique that emerged this quarter involved threat actors using Morse code to deliver phishing URLs to their victims. Due to its history of successful attacks, threat actors increased their use of RDP exploits this quarter to attack employees working from home. ZeroFOX also identified a new Cash App-themed phishing kit operated by the 16Shop kit distribution network, which successfully launched in February 2021 due to the popularity of Cash App.

Morse Code Phishing URL

Phishing threat actors are becoming more sophisticated with their delivery methods, using simple and evasive ways to deliver threats to targets. In Q1 2021, threat actors distributed phishing emails containing obfuscated code that delivered phishing URLs in Morse code.[8] Morse code is a type of encoding used in telecommunications where dots and dashes represent characters.[9] In the context of these phishing emails, threat actors spread HTML files, resembling a Microsoft Excel spreadsheet, that used JavaScript to map plaintext characters to corresponding Morse code characters. Figure 4 is an example of a Morse code HTML file.

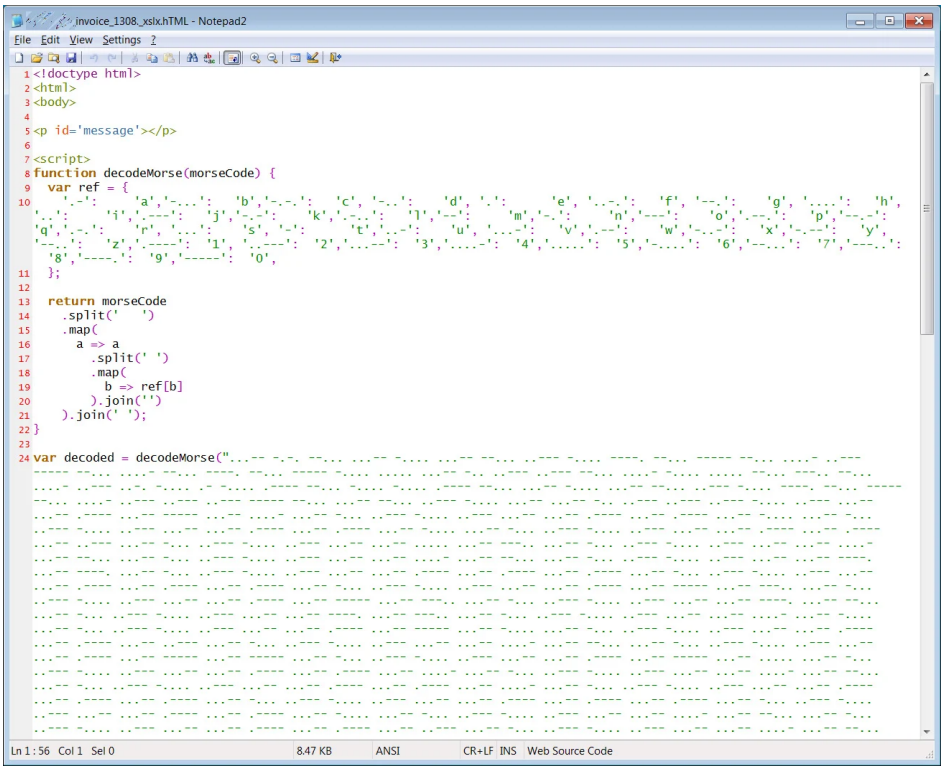


Figure 4: HTML source code of file delivering Morse phishing URL

Source:

hXXps://www[.]bleepingcomputer[.]com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/

The code structure in Figure 4 evades detection effectively. However, the actual phishing email is quite simplistic—the threat actors use a subject line referring to an invoice payment and include the recipient's company name but do not include a message body. This fact highlights that this phishing scam is a targeted attack, despite its simplistic look and feel. Clicking the attached file calls the decodeMorse() function, which converts the encoded string to hexadecimal and then into JavaScript tags to inject into the HTML. This then renders a fake Excel Online spreadsheet where the threat actors steal the recipient's Microsoft credentials.

16Shop Cash App Phishing Kit

Phishing distribution networks offer services whereby threat actors can easily and quickly deploy phishing websites by purchasing a customizable kit folder. 16Shop is one kit creator that offers detection avoidance techniques, such as the ability to encrypt messages that kit buyers can use in phishing emails. 16Shop kits are robust and sophisticated, and, although they target a small number of brands, the scale of these targets allows them to compromise numerous victims and their banking details. This quarter, ZeroFOX Research discovered advertisements for the addition of Cash App-themed kits in February 2021.[10] Cash App, a mobile payment

service, grew in popularity during 2020 and eventually became an appealing target for threat actors. The Cash App kit reflects the standard sophistication of 16Shop kits, but little else distinguishes it from other 16Shop kits.

RDP Exploits and Remote Working Environments

In Q1 2021, RDP exploits remained a persistent threat as attackers increased the volume of brute force RDP attacks on targets.[11] RDP exploits surged throughout 2020 due to COVID-19 and the transition to remote employment. Threat actors used RDP exploits to target individuals working from home using unsecured networks for business operations.[12] Using RDP exploits, threat actors intrude into target networks using legitimate login credentials rather than deploying malware to obtain sensitive information.[13] A misconfigured RDP can lead to attackers exploiting unsecured networks, stealing sensitive information, and possibly deploying a ransomware to inflict further damage to the system.

Competition in Underground Communities

ZeroFOX monitors activity in numerous underground communities, including forums, marketplaces, and encrypted chat networks. These communities offer a place for threat actors to buy and sell resources and form connections with other actors entirely under the guise of anonymity. However, as these communities accumulate more members, competition increases—and threat actors manipulate, spread misinformation, and expose members to thwart competition. Typically, when a threat actor joins these communities, they strive to earn the trust of other members. This may include engaging with other threat actors or selling tools and resources. Anonymity and security play a significant role in these illicit networks, and reputation is vital for gaining the trust of legitimate actors and removing untrustworthy members—such as scammers, security researchers, and law enforcement officials. Some forums have *Guarantors* to help threat actors buy and sell tools and services. The guarantor acts as a liaison to ensure the integrity of the transaction between seller and buyer. The guarantor's reputation allows for smooth business relationships between threat actors and keeps underground communities thriving so long as members adhere to the website's privacy and security rules. Figure 5 is a screenshot of a threat actor providing tips on avoiding scammers in encrypted chat networks.

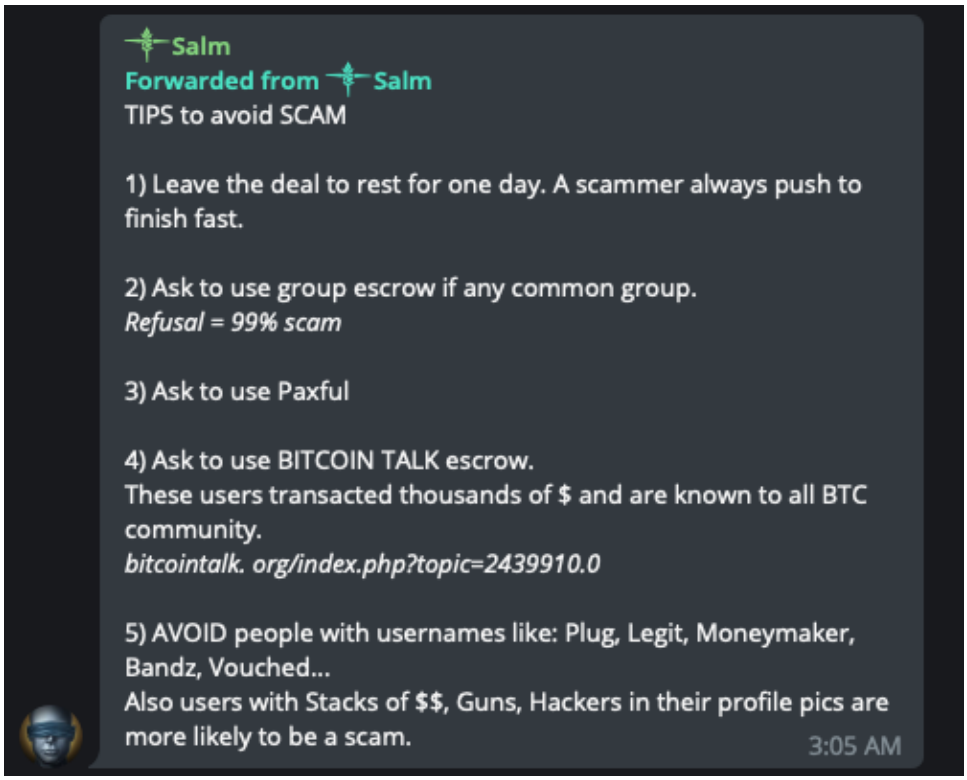


Figure 5: Tips on avoiding scammers in encrypted chat networks
Source: ZeroFOX Research

On the other hand, some threat actors expose community members to decrease competition and remove actors who pose a threat to the community. Threat actors are aware that law enforcement officers and security researchers have a presence in underground networks. While security researchers primarily visit these networks to collect intelligence, law enforcement efforts may lead to take downs and threat actor arrests. "Doxxing" is frequent in underground communities; some actors will post personal details on an actor or group, such as their name and location. Not only does the actor or group get exposed, but it also may be an opportunity for law enforcement to arrest actors. Doxxing also extends to researchers, law enforcement, or journalists. Operational security becomes imperative in these communities to preserve one's identity, especially as some threat actors attempt to cut down the competition via doxxing.

SolarWinds Orion Breach Overview

In December 2020, news broke that a large-scale supply chain attack occurred on the SolarWinds Orion platform, which impacted over 18,000 organizations in the commercial and federal space.[14] After SolarWinds disclosed the attack, security experts investigated the breach to determine which systems were affected and what threat actors were responsible. The primary malware identified during the initial breach investigation was Sunburst. However, after weeks of research, it is apparent that additional types of malware were used in conjunction with the Sunburst infection. Thus far, multiple malicious artifacts have been identified in the breach associated with the primary Sunburst infection or a standalone infection, such as the Supernova malware. The number of identified unique malware samples highlights the severity of the SolarWinds breach. More information continues to emerge indicating that the impact is more significant than what was initially reported. Figure 6 contains the current six identified malware types and a brief overview of their function as it relates to the SolarWinds incident.

Malware	Description
Sunburst	Primary malware used in SolarWinds Orion breach. Sunburst remains silent for two weeks before it receives commands to transfer data, execute files, disable services, and reboot the machine.[15]
Sunspot	Loader that injects Sunburst into SolarWinds Orion platform.[16]
Supernova	SuperNova is **not** part of the SolarWinds supply chain attack but was placed by attackers on a system that hosts SolarWinds Orion.[17]
Teardrop	Dropper malware that deploys a Cobalt Strike beacon; delivered by Sunburst backdoor.[18]
Raindrop	Loader malware that delivers Cobalt Strike beacon and spreads across victims' networks. Is not delivered by Sunburst and uses a custom packer to pack Cobalt Strike.[19]
Sunshuttle	Sophisticated second-stage backdoor for Sunburst that communicates with command and control locations and executes commands.[20]

Figure 6: Identified malware in the SolarWinds breach

Source: ZeroFOX Research

The United States (US) government believes Russian threat actors were responsible for the SolarWinds operation.[21] Some security researchers claim that Sunburst shares similar source code with the Kazuar backdoor, a malware linked to the Turla advanced persistent threat (APT) group.[22] However, the Kazuar malware is constantly updated with new code changes and

packing methods, which makes Sunburst less likely to be attributable to Turla. Some researchers believe that Chinese threat actors may also share responsibility. Currently, security experts assess that Russian threat actors compromised the SolarWinds Orion build environment to insert malware on the platform. Chinese threat actors are believed to have exploited a vulnerability in the Orion system but to have conducted the operation separately from the alleged Russian threat actor involvement.[23] As of this writing, both the Russian and Chinese governments deny responsibility for the attacks.

Top Vulnerabilities and Exploits

This quarter, new types of common vulnerabilities and exposures (CVEs) received significant attention due to the critical nature of their flaws and the resulting attacks carried out by threat actors, such as the Microsoft Exchange server attacks. Figure 7 highlights the volume of social media mentions of common vulnerabilities and exposures (CVEs) on a weekly basis captured by ZeroFOX Research this quarter. Charting this volume provides an overview of the public's interest in a CVE. The mentions may contribute to a CVE's severity level, capabilities, or general popularity.

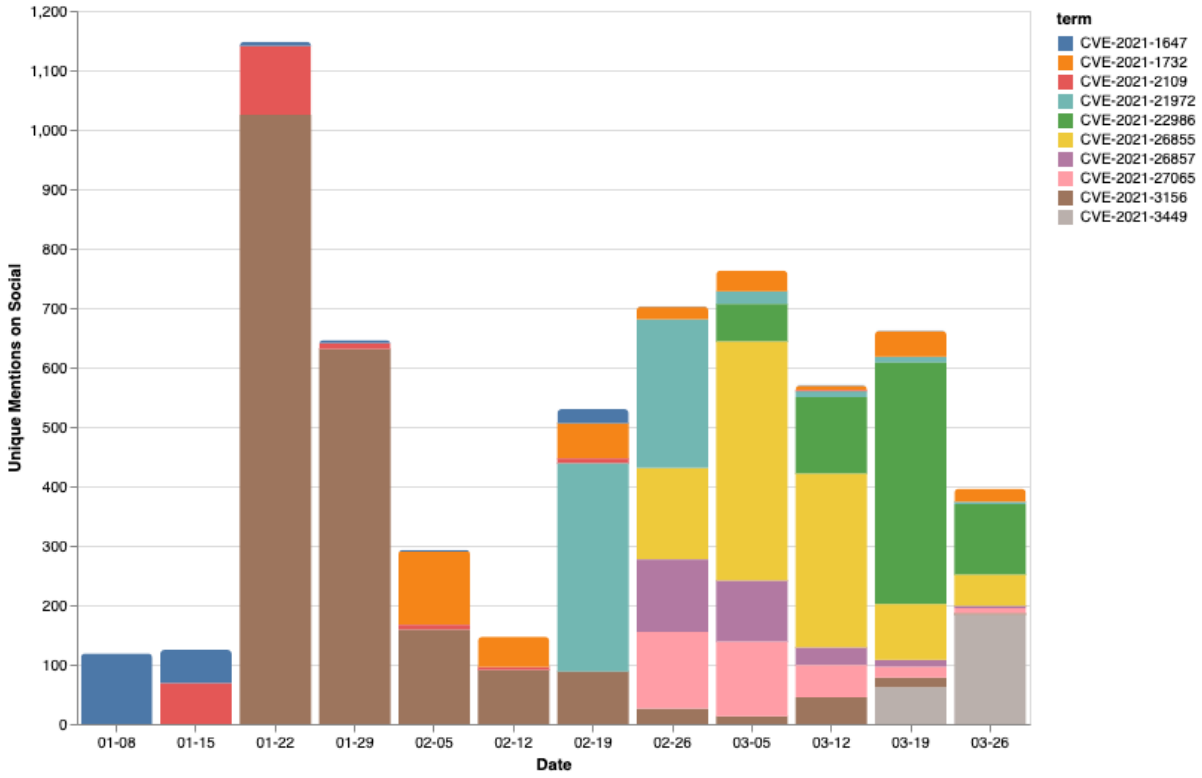


Figure 7: Identified mentions of common CVEs in Q1
Source: ZeroFOX Research

The highest volume of CVE mentions this quarter took place in January 2021 regarding CVE-2021-3156 (brown bar). This vulnerability is a buffer overflow flaw discovered in the sudo program (versions 1.9.5p2 and older) that allows privilege escalation to root.[24] Sudo is a program in Unix-like operating systems that allows users to run programs with superuser security privileges. The sudo program is incredibly powerful; if a threat actor exploits this vulnerability, they could gain unauthorized root privileges on a vulnerable host machine.

Another CVE with a high-volume of social media mentions this quarter is CVE-2021-22986 (green bar). This vulnerability is used to exploit unauthenticated remote code execution attacks in the BIG-IP iControl REST interface.[25] Threat actors attempted to exploit this flaw in a wave of attacks during March 2021. By exploiting this vulnerability, threat actors can execute arbitrary system commands, create or delete files, and disable services.[26]

Microsoft Exchange Server "Hafnium" Attack

One of the more impactful incidents this quarter was the Microsoft Exchange Server attack. In this attack, dubbed “Hafnium” by Microsoft, China-based threat actors exploited four distinct vulnerabilities in Microsoft Exchange Server. Three of the four vulnerabilities were captured in the weekly mentions depicted in Figure 7. This attack gave the actors access to email accounts and permissions to install malware to provide long-term access to target environments. Figure 8 describes the four vulnerabilities involved in the Hafnium attack.

CVE	Description
CVE-2021-26855 (Yellow bar in Figure 7)	Server-side request forgery flaw in Exchange that allows actors to send arbitrary HTTP requests and authenticate as the Exchange server.
CVE-2021-26857 (Purple bar in Figure 7)	Insecure deserialization vulnerability in the Unified Messaging service. The exploitation of this flaw allows attackers the ability to run code as "system" on an Exchange server and requires administrator permission or another vulnerability to exploit.
CVE-2021-26858	A post-authentication arbitrary file write vulnerability where attackers could write a file to any path on a target Exchange server by exploiting CVE-2021-26855 or compromise a legitimate administrator's credentials for authentication.
CVE-2021-27065 (Pink bar in Figure 7)	Vulnerability identical to CVE-2021-26858; arbitrary file write vulnerability where attackers could write a file to any path on a target Exchange server by exploiting

	CVE-2021-26855 or compromise a legitimate administrator's credentials for authentication.

Figure 8: CVEs identified in Hafnium attack
Source: hXXps://www[.]microsoft[.]com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Leveraging these vulnerabilities in the attack chain empowers attackers to execute remote code, steal data, load additional malware, or otherwise hijack the victim server.[27] Microsoft has released patches for affected systems; however, applying patches may not be enough to remove any additional malware installed by the Hafnium actors. As some security teams wrap up their investigation of the SolarWinds Orion breach, the Halfium attack brings forth a new set of issues for security professionals to address and mitigate. ZeroFOX Research observed a posting on a Russian-language forum in which an actor offered to buy working exploits of CVE-2021-26855 and CVE-2021-27065 for USD 50,000. Figure 9 displays the screenshot of the advertisement followed by an English translation of the Russian text.

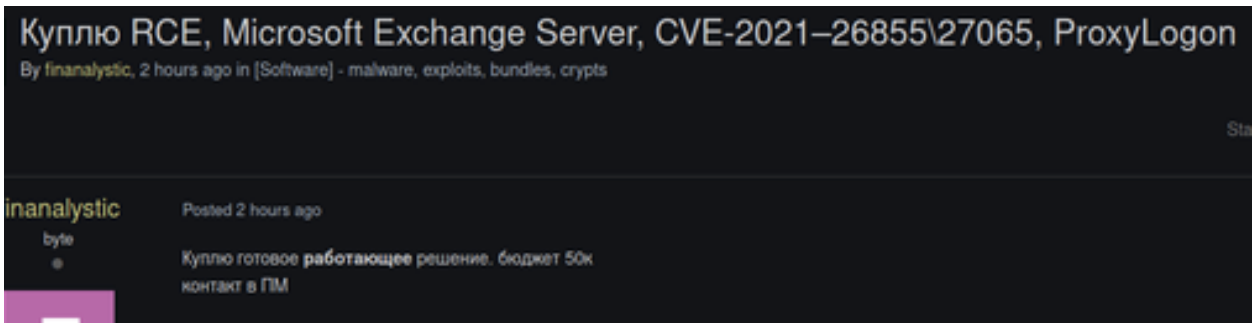


Figure 9: Actor advertises purchase of CVE-2021-26855 and/or CVE-2021-27065 on Russian-speaking forum
Source: ZeroFOX Research

English Translation:

> *Buy RCE, Microsoft Exchange Server, CVE-2021–26855 \ 27065, ProxyLogon*
> *I will buy a ready-made working solution. budget 50k*
> *contact in PM*

The breadth of this incident also involved ransomware attacks. Threat actors leveraged the Microsoft Exchange server vulnerabilities to install the DearCry ransomware on targeted environments.[28] DearCry immediately begins its encryption process when executed on Windows operating systems. When completed, the ransomware presents a demand note with instructions on paying the ransom to retrieve the decryption key. Another ransomware with a possible connection to the Exchange server attacks is the Hades ransomware.[29] Security researchers analyzed a Hades infection and identified a domain linked to a Hafnium command

and control location. The use of ransomware in conjunction with the Exchange server vulnerabilities underscores the severity of this attack. Security professionals urge Microsoft Exchange users to quickly patch these flaws before threat actors deploy follow up attacks on targets.

Industry Overview

Throughout 2020, key industries experienced various cyber threats due to COVID-19 affecting business operations and threat actors exploiting current events and remote employment. In 2021, these industries continue to face similar threats but with higher severity levels. ZeroFOX Research provides an overview of threats impacting four industries in Q1 2021.

Finance

As COVID-19 continues to impact businesses in the US and around the world, fraudsters take advantage of financial assistance programs offered to small businesses and individuals impacted by the pandemic. Beginning in 2020 and continuing in 2021, pandemic assistance fraud remains a threat to finance organizations. The U.S. Department of Labor estimates that more than **USD 63 billion** has been lost to pandemic-related financial fraud in the US.[30] Essentially, this scheme involves threat actors obtaining stolen personal identifying information from underground networks and using that data to file false claims to receive pandemic financial assistance. Much of this activity exists in encrypted chat networks where scammers publish tutorials on conducting pandemic fraud scams, sell data for scammers to buy, and post evidence of successful scam payouts. ZeroFOX Research retrieved a post made in a chat network in which threat actors abuse Small Business Administration-related pandemic relief. Figure 10 is an advertisement selling methods for obtaining loans and other financial assistance.

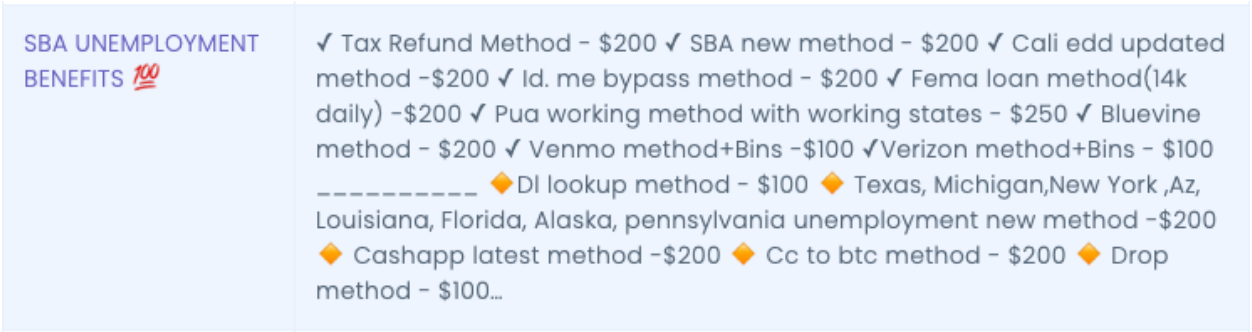


Figure 10: Scammer selling methods for financial fraud scams
Source: ZeroFOX Research

Another category of financial scams this quarter is the exploitation of COVID-19 stimulus payments and tax-filing season. The U.S. Department of Treasury warns individuals about scammers using COVID-19-themed threats to extract personal and financial information from potential targets and requests that they contact the Federal Bureau of Investigation for assistance.[31] As these scams persist, resulting in billions of dollars lost to threat actors, law enforcement officials track scammers and investigate instances of fraud. The Department of Justice indicted individuals accused of pandemic relief fraud and monitors fraud activity surrounding stimulus payments and tax-filing season.[32]

Pharmaceutical

The pharmaceutical industry continues to experience instances of vaccine-related threats as nations around the world distribute the COVID-19 vaccine to eligible recipients. Threat actors sell false COVID-19 vaccines on scam websites and cyber criminal marketplaces and publish vaccine-related data leaks obtained from pharmaceutical companies. The U.S. Department of Health and Human Services issued a warning to individuals about vaccine scams, urging them not to purchase vaccines or other treatment options from these sellers and to avoid posting vaccination record cards on social media.[33] ZeroFOX Research retrieved instances of threat actors selling vaccines on underground marketplaces, including a market called "Corona Market" selling treatment vaccines (Figure 11).

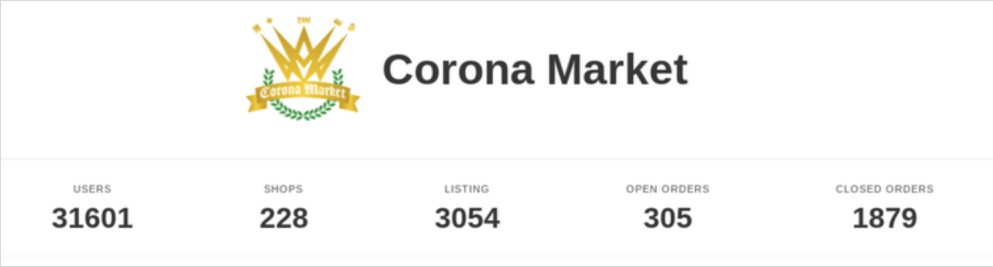


Figure 11: Corona Market logo and shop statistics
Source: ZeroFOX Research

Threat actors are also deploying phishing websites using a vaccine theme to steal victim's personal information. Law enforcement officials issued take downs on phishing websites hosted on domains impersonating the names of pharmaceutical organizations and COVID-19 treatment drugs.[34] Capitalizing on the COVID-19 vaccine distribution is a lucrative scam tactic for threat actors as the public waits to receive vaccinations.

Industrial Control Systems

In February 2021, a threat actor obtained unauthorized access to an internal industrial control systems (ICS) platform for a Florida water treatment facility and attempted to change the water's chemical levels, making it undrinkable. The attack was quickly mitigated once facility operators learned of the incident. The resulting investigation found that the threat actor accessed the plant's supervisory control and data acquisition (SCADA) system using the TeamViewer remote access software, likely via a compromised password.[35] The investigation also found that the plant's system was hosted on an outdated operating system, which may have contributed to the attack.

One of the biggest takeaways from this incident is the importance of securing operational technology (OT) in ICS organizations. Unlike information technology (IT), which primarily refers to computing technology, OT refers to hardware technology and is industry-oriented. While it is easier to update and secure IT systems, it is difficult to do the same with OT systems. OT networks are older, which makes updating these networks a time-consuming and complex task. Although it may seem that the solution to avoid a similar attack is that ICSes should not allow remote access to plant infrastructure, the primary issue is that ICSes do not have the resources to support updating systems and networks to function fully-remote and securely.

Retail

As a result of COVID-19 in 2020, the retail industry exhibited increased sales due to a surge in online shopping. However, this surge also brought forth a broader attack surface for threat actors to exploit. In 2021, e-commerce activity continues to grow and evolve, requiring retailers to rethink e-commerce security to protect their organization and their customers.[36] Protecting customer data is one of the biggest challenges as retailers attempt to mitigate data leaks and fraud risks. The data-rich information stored on retailers' internal systems appeals to threat actors, as they can steal that data to conduct additional nefarious activities. This information's importance requires retailers to be mindful of data storage security to prevent threat actors from accessing this information. Network segmentation may provide some security in keeping customers' personal and financial information secure.

Another trend for e-commerce cybersecurity is that some threat actors are pivoting from using point of sale malware to using digital credit card skimmers. While physical skimmers require hardware to fit over payment terminals, digital skimmers inject malicious code into online payment systems. These digital skimmers allow threat actors to use evasive techniques and code obfuscation that prevent some online security technologies from detecting malicious

activity. The threat of e-commerce malware challenges retailers to use malware detection software that alerts on the presence of malicious code on networks. In addition, applying security updates and patches to outdated or flawed software prevents threat actors from exploiting vulnerabilities in systems.

Conclusion

The evolution of the global cyber threat landscape continues in 2021 after a quarter rife with cyber activity. Although many of the threats observed in 2021 are a continuation of 2020's cyber activity, threat actors used a combination of historically successful techniques with new tactics to spread threats to their victims evasively. While the collaboration of international law enforcement offices resulted in the disruption of high-profile cybercrime operations, it is unclear if and when threat actors will shift to another source for nefarious activity. New exploit and vulnerability disclosures brought forth highly severe attacks on corporate systems, including attacks against Microsoft Exchange server. Meanwhile, cyber underground communities exhibited an increased number of threat actors entering a heavily competitive cybercrime market. Furthermore, as the COVID-19 vaccination efforts continue worldwide, threat actors also continue to find ways to exploit the pandemic and target employees working from home with cyber threats. While it is unclear what the threat landscape will endure in the remainder of 2021, Q1 provided a glimpse into what can be expected of cyber threat and threat actor activity.

Sources

1 hXXps://www[.]europol[.]europa[.]eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

2 hXXps://www[.]zdnet[.]com/article/jokers-stash-the-internets-largest-carding-forum-is-shutting-down/

3 hXXps://squareup[.]com/us/en/townsquare/what-is-a-card-not-present-transaction

4 hXXps://www[.]zdnet[.]com/article/egregor-ransomware-operators-arrested-in-ukraine/

5 hXXps://www[.]zdnet[.]com/article/new-trickbot-module-uses-masscan-for-local-network-reconnaissance/

6 hXXps://www[.]zerofox[.]com/blog/maze-recent-ransomware-attacks/

7 hXXps://www[.]darkreading[.]com/endpoint/interview-with-a-russian-cybercriminal/d/d-id/1340029

8 hXXps://www[.]bleepingcomputer[.]com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/

9 hXXps://www[.]britannica[.]com/topic/Morse-Code

10 hXXps://www[.]zerofox[.]com/blog/16shop-cash-app-phishing-kit/

11 hXXps://www[.]darkreading[.]com/threat-intelligence/rdp-attacks-persist-near-record-levels-in-2021/d/d-id/1340444

12 hXXps://www[.]helpnetsecurity[.]com/2021/02/12/rdp-attack-attempts-surge/

13 hXXps://www[.]zdnet[.]com/article/big-jump-in-rdp-attacks-as-hackers-target-staff-working-from-home/

14 hXXps://www[.]cisa[.]gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

15 hXXps://www[.]solarwinds[.]com/sa-overview/securityadvisory

16 hXXps://www[.]bleepingcomputer[.]com/news/security/new-sunspot-malware-found-while-investigating-solarwinds-hack/

17 hXXps://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar21-027a

18 hXXps://symantec-enterprise-blogs[.]security[.]com/blogs/threat-intelligence/solarwinds-raindrop-malware

19 Ibid[.]

20 hXXps://www[.]zdnet[.]com/article/microsoft-weve-found-three-more-pieces-of-malware-used-by-the-solarwinds-attackers/

21 hXXps://www[.]reuters[.]com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R

22 hXXps://threatpost[.]com/solarwinds-hack-linked-turla-apt/162918/

23 hXXps://www[.]reuters[.]com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8

24 hXXps://cve[.]mitre[.]org/cgi-bin/cvename[.]cgi?name=CVE-2021-3156

25 hXXps://cve[.]mitre[.]org/cgi-bin/cvename[.]cgi?name=CVE-2021-22986

26 hXXps://support[.]f5[.]com/csp/article/K03009991

27 hXXps://www[.]zdnet[.]com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

28 hXXps://www[.]bleepingcomputer[.]com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/

29 hXXps://threatpost[.]com/hades-ransomware-connections-hafnium/165069/

30 hXXps://apnews[.]com/article/pandemics-health-coronavirus-pandemic-asia-pacific-ohio-b651def05a8a049637c4a1047f788631

31 hXXps://home[.]treasury[.]gov/services/report-fraud-waste-and-abuse/covid-19-scams

32 hXXps://www[.]justice[.]gov/usao-vi/pr/warning-issued-us-attorney-and-irs-criminal-investigation-pertaining-new-wave-covid-19

33 hXXps://oig[.]hhs[.]gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/

34 hXXps://www[.]bleepingcomputer[.]com/news/security/us-seizes-more-domains-used-in-covid-19-vaccine-phishing-attacks/

35 hXXps://www[.]cyberscoop[.]com/florida-water-facility-hack-password/

36 hXXps://securityintelligence[.]com/articles/shift-e-commerce-how-retail-cybersecurity-is-changing/