



Quarterly Threat Landscape Review

Q2 2021

Table of Contents

Executive Summary	3
Key Points	3
Evolving Threats of Ransomware and Malware	4
Superscale Ransomware Attacks	4
Major Ransomware Trends and Takedowns	5
Other Malware Trends	8
The Effect of Underground Networks on Government Targets	9
Aftermath of SolarWinds Breach on Underground Marketplaces	9
ZeroFox Metrics on Ransomware Targeting Government Offices	10
Legislation to Improve National Cybersecurity Response	12
Breaking Down the Phishing Ecosystem	14
Source Code and Phishing Kits	14
Lure Distribution Mechanisms	15
Third-Party Services and APIs	16
Retail-targeted Phishing	17
Finance-targeted Phishing	17
Selling Victim Data	18
Top Vulnerabilities and Exploits of Q2 2021	19
CVE-2021-1675: A Case of Earnest Misinformation	22
CVE-2021-21985: Vulnerable vCenter Services Offer Foothold Into Organizations	24
CVE-2021-31166 - Wormable RCE in Windows HTTP Stack	26
Recommendations	27
Conclusion	28

Executive Summary

In the second quarter of 2021 (Q2), threat actor tactics, techniques, and procedures (TTPs) reflected that of the evolving threat landscape which included increased activity from ransomware attacks, severe security vulnerabilities, and legislation addressing cyber attacks. Increasing levels of ransomware attacks took place this quarter, demonstrating the evolving and critical threat such attacks pose to organizations and individuals. As a result of these ransomware attacks, as well as other high-impact cyber attacks on United States (US)-based organizations, President Joe Biden issued a presidential executive order creating a plan to address cyber attacks in order to strengthen national security. In terms of cyber criminal underground networks, ransomware played a significant role in marketplace networks, as threat actors launched new data leak websites and advertised compromised data to profit from ransomware attacks. As phishing attacks remain a consistent threat, phishing ecosystems provide context on successful operations and how threat actors leverage stolen data from attacks. The new vulnerabilities and exploits that emerged this quarter have the potential to critically impact enterprise organizations, such as the PrintNightmare vulnerability that can allow attackers to run arbitrary code with SYSTEM privileges. In this Quarterly Threat Landscape Review, ZeroFox Threat Research provides an overview of the threats that impacted the global threat landscape in Q2 2021.

Key Points

- Ransomware attacks increased by 50 percent this quarter, as more types of ransomware emerged on the threat landscape and caused significant damage to affected victims.
- In response to high-profile cyber attacks like ransomware, President Biden enacted legislation through Executive Order 14028 to improve national cybersecurity after the Colonial Pipeline attack caused fuel shortages in parts of the country.
- The increased public scrutiny of cyber criminal underground networks, especially ransomware groups, due to arrests, asset seizures, and website takedowns caused some groups to disappear this quarter, while new ones emerged or others increased operations.
- Marketplace networks for phishing and fraud-related activities enable threat actors to obtain lucrative profits by creating, operating, and selling stolen data. Phishing supply chains present a comprehensive ecosystem for threat actors to create and operate tools and data for profit from credential phishing attacks.

- New vulnerabilities and exploits disclosed this quarter included a security flaw dubbed PrintNightmare (CVE-2021-34527) that allows threat actors to remotely access a target domain controller to execute commands and deploy malware on the system.

Evolving Threats of Ransomware and Malware



Malware



Internet Infrastructure

Superscale Ransomware Attacks

This quarter, the number of ransomware attacks are greater than ZeroFox Threat Research has ever observed, and the scale of those attacks in terms of victims has grown to unprecedented levels. In May, the ransomware group Darkside encrypted key segments of the network at Colonial Pipeline, including the systems that managed the gasoline and jet fuel transportation lines.¹ Even after quickly paying the USD 4.4M ransom, gas shortages affected large segments of the country, exposing dangerous vulnerabilities in critical components of the infrastructure of the US. The attack appeared to exceed the intentions of the attacker, and the severity of the attack sent shockwaves through the nation and was enough to cause many in the hacker community to express frustration with the attack, worrying that it drew too much unwanted attention to their activities.

Likewise, in what was likely the largest scale single ransomware attack ever, managed services provider Kaseya was attacked by REvil, who first penetrated Kaseya's systems and then reportedly leveraged that access to cascade their attack onto Kaseya's customers.² It is estimated that the attack compromised between 800 and 1,500 companies, and, according to the attacker, affected one million systems. Unlike Darkside, who immediately attempted to mitigate the international scrutiny their attack had drawn, REvil publicly revelled in their achievement, allegedly demanding a USD 70 million ransom payment initially, though reports also state that they later revised that demand to USD 50 million.

¹ <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>

² <https://www.zdnet.com/article/kaseya-ransomware-attack-what-we-know-now/>

These attacks illustrate the potential scale and impact that ransomware can have beyond the targeted companies and their customers. It will likely take quite some time before attacks of this magnitude can become common, but given that such attacks have already occurred and proven successful, it is reasonable to assume that attackers will continue to push those boundaries unless some action is taken to stop them.

Major Ransomware Trends and Takedowns

Increased takedowns and law enforcement intervention is an ongoing trend with regard to ransomware, malware, and the services that host them. In previous quarters, authorities have seized servers, arrested members, or otherwise disrupted operations for TrickBot, Emotet, Egregor, and NetWalker. These teams represent some of the largest players in malware and ransomware.

During the current quarter, an affiliate of Darkside (although not Darkside themselves) was arrested and taken offline in May.³ In June, the prolific ransomware actor Avaddon shut down their operation and sent thousands of decryption keys for their current victims to BleepingComputer. Authorities in Ukraine also arrested six members of the Cl0p ransomware group and seized several servers.⁴

The question then becomes: is it making a difference?

Month over month, ZeroFox observed numbers above 235 ransomware attacks on average per month this quarter, based on data leak website exposure. More specifically, in April we observed 227, in May we observed 258, and in June we observed 221. It could be argued that the attack rate is increasing based on the average number of attacks per day - 7.57 attacks per day in April, 8.32 attacks per day in May, and 7.37 attacks per day in June. However, these attacks are often released in groups, and that small trend may not be significant in isolation.

How does that fare in comparison to previous quarters? This quarter we saw a marked *increase* in ransomware attacks, moving up from a monthly average of just over 150 per month. There were 128 in January, 179 in February, and 157 in March, equating to 4.13, 6.39, and 5.06 average attacks per day; this is an approximately 50 percent increase in a single quarter. This data is reflected in Figure 1.

³ <https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-operation-shuts-down/>

⁴ <https://www.darkreading.com/attacks-breaches/ukraine-police-disrupt-cl0p-ransomware-operation/d/d-id/1341323>

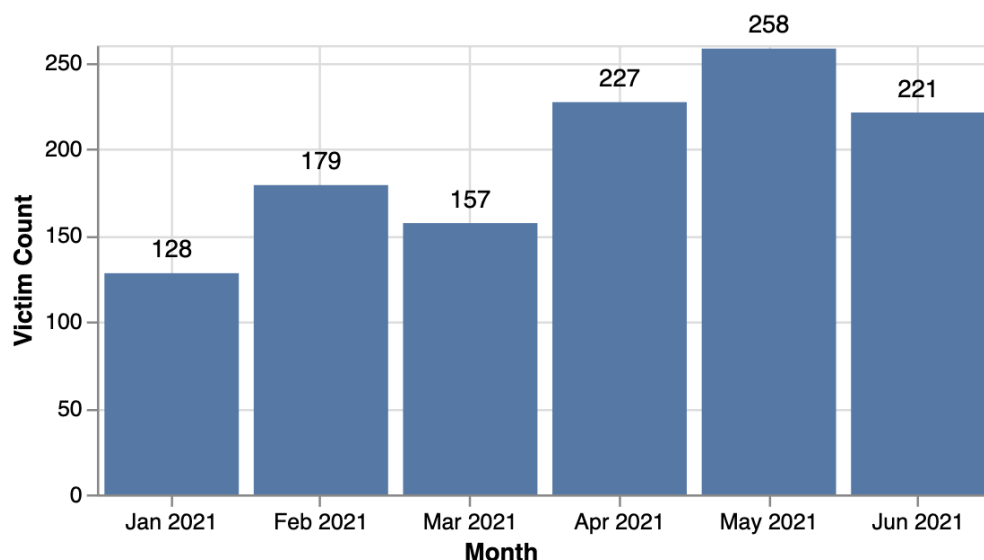


Figure 1: Monthly Number of Ransomware Attacks
Source: ZeroFox Threat Research

There is clear evidence that major disruptions occurred within some of the biggest threat actor groups this quarter. After the Colonial Pipeline attack, Darkside and several other actors took very public steps to draw back their operations and promised to exclude entire industries—in addition to working harder to vet the work of their affiliates— and then shut down completely. Avaddon was an active and prolific attacker before they shut down their operation. As mentioned previously, several members of the CI0p team in Ukraine were arrested, and their local systems were seized. All three of these actors were among those who attacked the greatest number of ransomware victims this quarter.

ZeroFox Threat Research also observed additional disruptions, such as:

- One of the most popular "bulletproof" VPN services, DoubleVPN – a favorite amongst threat actors – was seized by law enforcement officials.⁵
- A similar seizure was performed in December against common bulletproof providers insorg[.]org, safe-inet[.]com, and safe-inet[.]net.⁶
- A free file decryptor for victims of Lorenz ransomware was released by researchers in June.⁷
- The source code for Paradise ransomware was leaked in May.⁸
- A central distributor for Gozi, a Romanian by the name of Mihai Ionut Paunescu, was arrested in Columbia on charges in the US.⁹

⁵ <https://www.reuters.com/technology/doublevpn-service-used-by-hackers-seized-shut-down-2021-06-30/>

⁶ <https://www.zdnet.com/article/law-enforcement-take-down-three-bulletproof-vpn-providers/>

⁷ <https://www.bleepingcomputer.com/news/security/lorenz-ransomware-decryptor-recovers-victims-files-for-free/>

⁸ <https://www.bleepingcomputer.com/news/security/paradise-ransomware-source-code-released-on-a-hacking-forum/>

⁹ <https://www.infosecurity-magazine.com/news/gozi-virus-arrest-made-in-columbia/>

Despite all these actions and more, both the sheer number of ransomware attacks and the rate at which the ransoms are paid seem to continually grow. Two ransom demands against personal computer manufacturers Acer and Quanta, a supplier for Apple computers, have reached USD 50 million.¹⁰ The average ransom payment has scaled to over USD 220 thousand according to ransom researchers.¹¹ The partial takedown against Cl0p was a short-lived victory, with the actor advertising a successful attack against a new victim the very next week. Even with these disruptions, 75 percent of the attacks that ZeroFox Threat Research monitored were performed by ten actors. A breakdown by actor is shown in Figure 2.

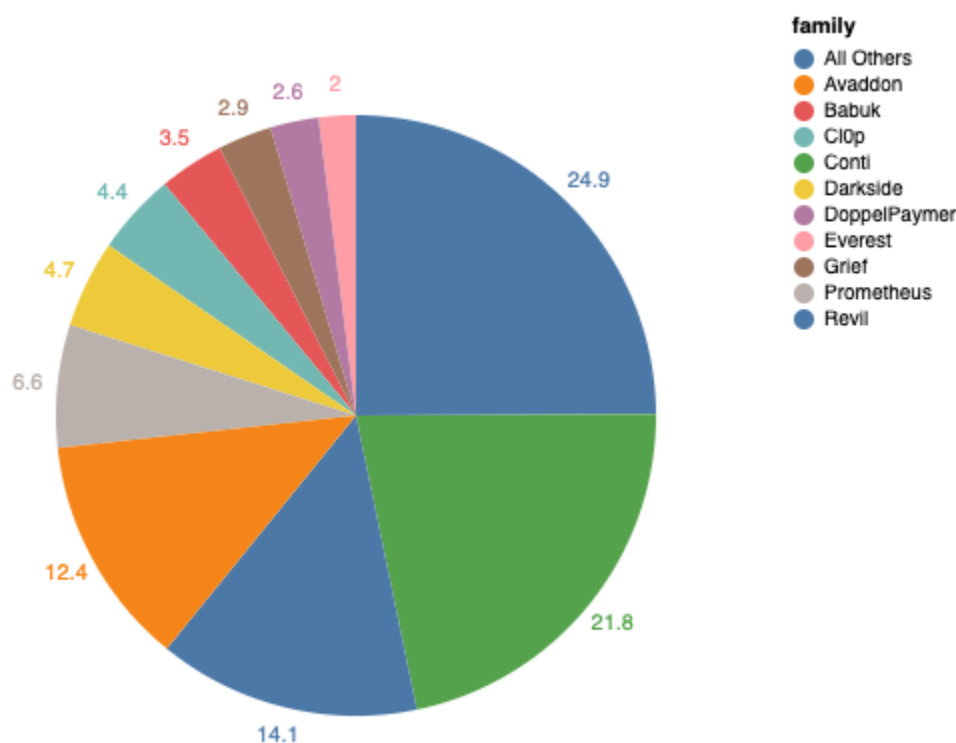


Figure 2: Percentage of Ransomware Attacks by Threat Actor
Source: ZeroFox Threat Research

There are, however, positive signs that the ransomware operators are feeling pressure. In the wake of the Colonial Pipeline attack, several actors other than Darkside publicly stated that there would be boundaries and limits on what was acceptable, and several popular criminal underground forums banned discussions relating to ransom auctions.¹² Ransomware operator Babuk closed its affiliate program, rebranded their leak site as payload[.]bin, and focused their public presence to emphasize "pen testing." To further confuse the picture, Babuk 2.0 launched

¹⁰ <https://www.theverge.com/2021/4/21/22396283/apple-schematics-leak-ransomware-quanta-supplier-leak>

¹¹ <https://www.cyberscoop.com/ransomware-extortion-demands-increasing-coveware/>

¹² <https://www.bleepingcomputer.com/news/security/ransomware-ads-now-also-banned-on-exploit-cybercrime-forum/>

in July 2021.¹³ Actor group Evil Corp, associated with Dridex, BitPaymer, and WastedLocker, also began referring to itself as PayloadBin, presumably in an effort to sow confusion.¹⁴ Similarly, the operators of PwndLocker ransomware changed their name to ProLock in March 2021.

The ransomware tools themselves are becoming pivot points. A builder for Babuk ransomware was leaked in June. An unknown actor appears to have edited REvil's binaries in a hex editor and leveraged them for their own attacks. Trickbot, a group that sees their tool leveraged by a large number of attackers and that has been targeted in multiple large takedown efforts, changed direction slightly in July 2021 and released a new banking module, possibly signaling a need to redirect their business back into more familiar territory.¹⁵

Other Malware Trends

While ransomware dominated the security headlines this quarter, it was not the only malware threat on the landscape. Zeus infections continue to be an ongoing and growing threat. Mirai botnets received an upgrade this quarter and are on the rise as well. New versions of Agent Tesla RAT surfaced near the beginning of the quarter, and Metasploit Meterpreter and Cobalt Strike continue to be heavily leveraged in several different kinds of attack. Even long-time data skimmer Magecart's activity surged this quarter.¹⁶

The activities of other threat actors may garner less attention than ransomware, because their attack methods may not be as destructive, have the same financial impact, or be as apparent, but such groups are still active and successful.

¹³ <https://www.bleepingcomputer.com/news/security/leaked-babuk-locker-ransomware-builder-used-in-new-attacks/>

¹⁴ <https://www.bankinfosecurity.com/blogs/evil-by-different-name-cybercrime-gang-rebrands-malware-p-3053>

¹⁵ <https://threatpost.com/trickbot-malware-virtual-desktop-espionage/167789/>

¹⁶ <https://thehackernews.com/2021/07/magecart-hackers-hide-stolen-credit.html>

The Effect of Underground Networks on Government Targets



I Deep Dark Web & Criminal Underground

Threat actors have used cyber criminal underground networks for illicit activities for years. With the recent increase in ransomware attacks, these networks are even more popular for buyers and sellers of stolen data. Along with countless other victims and verticals, various US government entities had their data listed for sale, or offered for free, on popular underground marketplace forums for anyone to purchase and analyze.

ZeroFox researchers observed more local and state governments becoming victims, with ransomware being the main threat in recent months. By using these underground marketplaces, threat actors can "name and shame" victims into paying ransom demands, disclosing stolen data, or preventing access to their data, since it is rather trivial for ransomware groups to create new infrastructure to host these types of sites, even if taken down by authorities. This quarter, ZeroFox Threat Research observed actors attempting to buy access to government agencies through Citrix virtual private networks (VPN) and remote desktop protocol (RDP), as well as brokers attempting to sell their access to government organizations.¹⁷

Aftermath of SolarWinds Breach on Underground Marketplaces

As the US continues to recover from the impact of the SolarWinds breach and the disclosure of new victims, data obtained from the breach made its way to marketplace forums for sale and distribution. ZeroFox Threat Research observed one threat actor on a popular underground forum advertising a collection of 230 million US citizens' records reportedly stolen from the NSA due to the SolarWinds breach (Figure 3). However, this is most likely not legitimate. Even in cases where the data may not be legitimate, attackers can still attempt to sell this data and capitalize on threat actors anxious to acquire the data.

¹⁷ <https://www.zerofox.com/blog/monitoring-network-access-sales/>

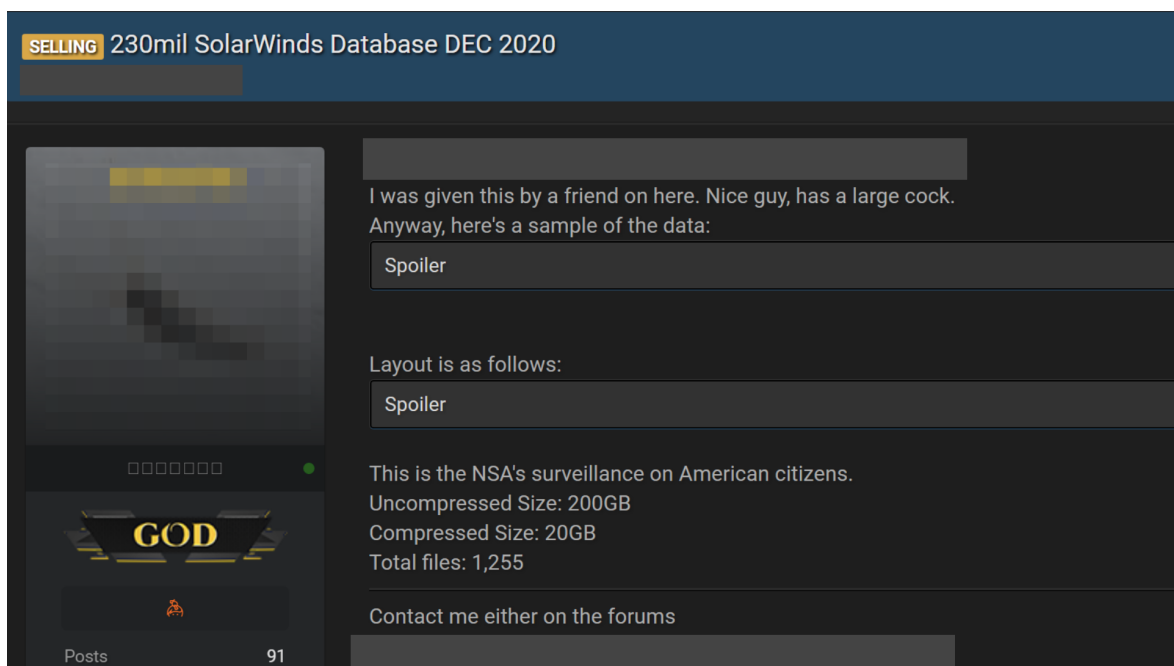


Figure 3: Actor advertising the sale of data allegedly obtained from the SolarWinds breach
Source: ZeroFox Threat Research

One of the largest threats observed by ZeroFox as it relates to cyber criminal underground networks is ransomware operators quickly and easily selling data from US government organizations. ZeroFox Threat Research observed multiple listings for this type of data. By leveraging marketplace networks, these threat actors can remain anonymous and sell data and tools with little risk. In addition, news agencies quickly report on stories of organizations being breached or infected with ransomware, which increases the victims' urgency to remedy the situation as quickly as possible.

ZeroFox Metrics on Ransomware Targeting Government Offices

Over this quarter, ZeroFox researchers tracked ransomware operators targeting government organizations on underground networks and identified 36 victims from these sites. Of these 36 victims, about 42 percent of the victims were located in the US or Canada. There are around 16 actively collected ransomware leak sites that presently contain victim data, with the most active ransomware groups targeting government agencies, including:

- Avaddon (22%)
- DoppelPaymer (13%)
- Conti (11%)
- Grief (8%)
- Everest (5%)

ZeroFox Threat Research expects that the number of "name and shame" websites on cyber criminal underground networks will increase, as this model has had relative success. In addition, we expect the number of victims, especially those in government, to rise quarter over quarter. This is due to the fact that these government organizations lack adequate funding to mitigate certain risks associated with malware and ransomware, and threat actors understand this. Lastly, with more ransomware operators and access brokers conducting activity on marketplace networks, there is an increased risk based on the sheer number of operators and brokers.

Figure 4 displays an example of the Marketo marketplace, a marketplace that offers to sell data from compromised companies and which has a listing for the Municipal Court of Princeton, West Virginia. In this posting, the actors specifically claimed that the court failed to protect the data of its citizens, stating "After this the reputation of Princeton Municipal Court and of the entire US judicial system will finally fly off in terms of security."

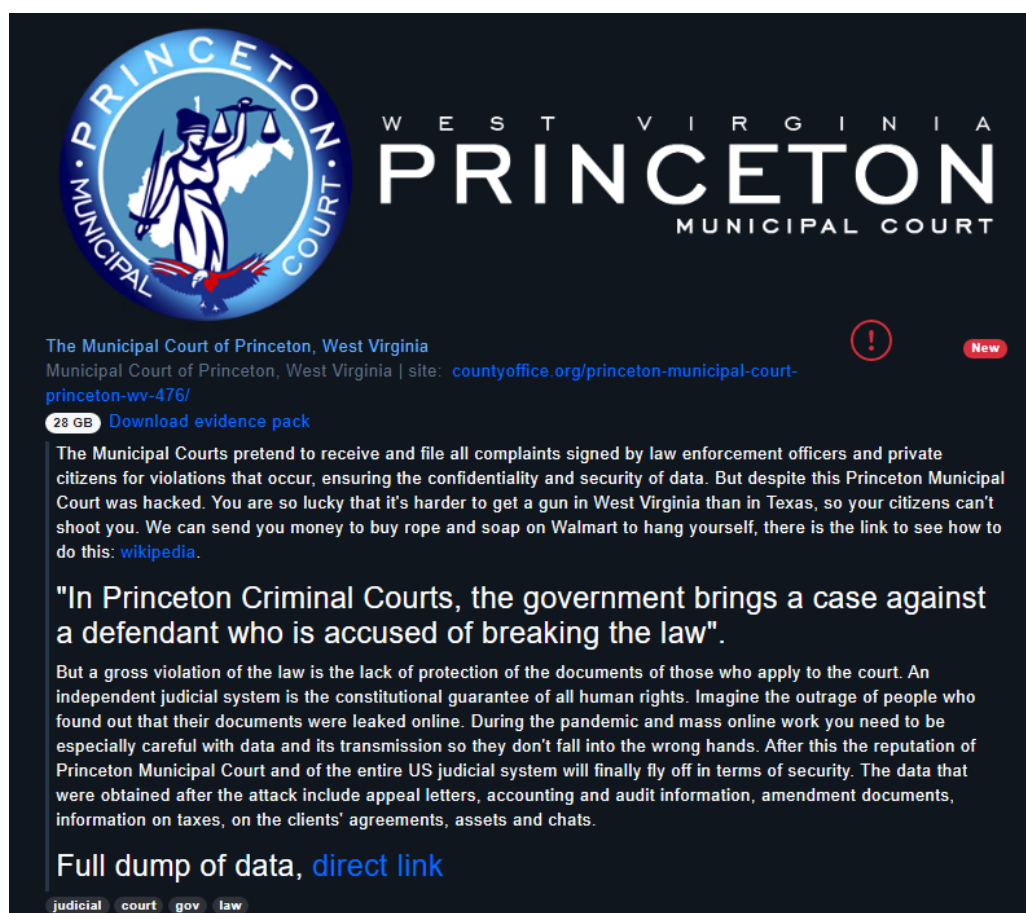


Figure 4: Marketo Marketplace listing for data from Municipal Court of Princeton
Source: ZeroFox Threat Research

As part of ZeroFox Threat Research's ongoing tracking of ransomware groups on underground networks, we have observed fluctuating ransomware infection rates on a weekly basis. The highest volume of attacks this quarter was during the week of May 30, 2021, when there was an increase in Pysa ransomware attacks, followed by Avoddon and Conti. The lowest volume of attacks occurred during the week of June 27, 2021, with 23 attacks. Figure 5 is a bar chart displaying the number of victims of ransomware and digital extortion by week in Q2 2021.

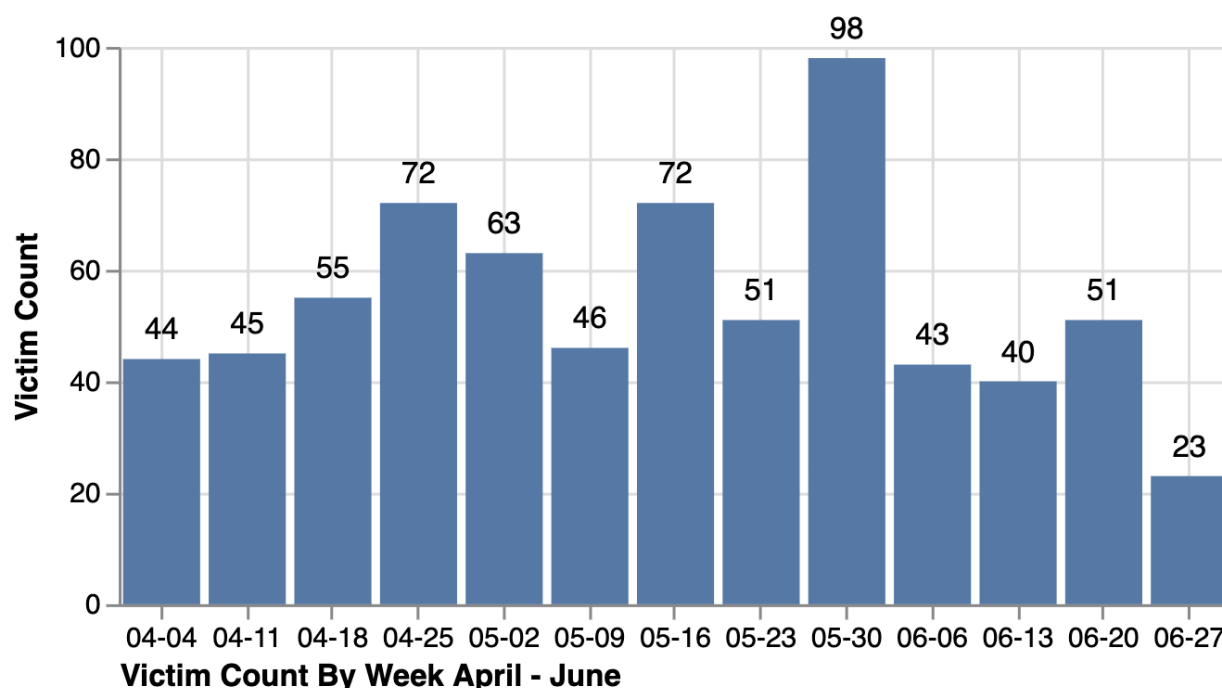


Figure 5: Ransomware and Digital Extortion by Week

Source: ZeroFox Threat Research

Legislation to Improve National Cybersecurity Response

| Geopolitical & Physical

From the SolarWinds Orion breach to Microsoft Exchange Server vulnerabilities to continuous ransomware attacks, cybersecurity becomes more important as the number of attacks increases daily. Thus far in 2021, organizations around the world have been impacted by various cyber threats, and this trend demonstrates that threat actors will not cease activity any time soon. This quarter, increased ransomware attacks on organizations prompted the US federal government to create a response plan to bolster national cybersecurity. Attacks like those against Colonial Pipeline, JBS, and Kaseya underscored the evolving threat of ransomware. Threat actors utilizing supply chain attacks and zero-day exploits demonstrate the

creative ways in which ransomware attacks become more dangerous to vulnerable targets. By issuing such legislation, the federal government can create an effective strategy to circumvent some cyber attacks.

One piece of legislation in question is the White House Executive Order aimed at improving US national cybersecurity.¹⁸ The order consists of eleven sections; eight of the sections provide a detailed plan to address the current struggle in preventing cyber attacks. Section Two of the order emphasizes the importance of removing barriers to share information, specifically through means like threat intelligence.¹⁹ After an organization or security experts disclose a cyber attack, security teams work quickly to hunt for any and all types of information on the incident—such as indicators of compromise, TTPs, or an analysis of the attack. Collecting this information typically helps other organizations understand how the attack occurred and how to decrease the chances of becoming compromised through a similar attack method. This is especially critical for supply chain attacks, referenced in Section Four of the order, which may become more prevalent due to the success of similar attacks in 2021.

Some sections in the executive order are specific to the federal government's response to cybersecurity incidents. The SolarWinds Orion breach demonstrated how a carefully planned attack could compromise over 18,000 organizations in the US and worldwide, and some of the affected organizations were government offices. The effects of the Colonial Pipeline attack further underscored how a single cyber attack can affect the general public and the economy, as well as the importance of securing critical infrastructure. These factors are crucial when it comes to improving cybersecurity on a national level. Section Six of the executive order discusses the federal government's role in creating a standardized playbook for responding to cybersecurity incidents and vulnerabilities. As more threat actors leverage zero-day flaws to conduct cyber attacks on organizations that use enterprise software and operating systems, the need to standardize a prevention and response plan becomes of the utmost importance.

This quarter further demonstrated how threat actors are using various tools in their arsenal to compromise businesses and government offices through cyber attacks. Although ransomware is one of the current top threats to organizations, it is one of many types of threats that can critically impact businesses. Ultimately the goal of this executive order is to push the federal government to take a stronger stance on cybersecurity. However, the implementation of such plans will reveal the effectiveness of the strategy.

¹⁸<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

¹⁹ <https://www.zerofox.com/blog/executive-order-on-cybersecurity/>

Breaking Down the Phishing Ecosystem



| PII & Fraud



| Brand

Phishing attacks aimed at consumers are commonly split into two buckets: conventional phishing and targeted spear phishing. Spear phishing is generally considered to be the more sophisticated type of attack, having specific targets; most conventional phishing is seen as lower-level activity, targeting indiscriminately and having a low success rate.

However, behind many typical phishing campaigns is a supply chain designed to facilitate these attacks and return a profit for those perpetrating them. Across dark web marketplaces and covert channels, buyers and sellers trade source code, victim data, access to services and tools disguised as legitimate services, and specialist equipment to scale phishing attacks beyond an individual threat actor's capability.

Source Code and Phishing Kits

Before beginning a phishing attack, the threat actor must obtain or create the code to render the phishing page to the victim. This commonly involves the threat actor obtaining an archive (.zip) containing pre-compiled code and resources, commonly referred to as a phishing "kit." This kit can be easily deployed to a web host to create a phishing page. These kits are bought and sold via various channels, with more sophisticated threat actors authoring kits based on demand.

Phishing kits can vary dramatically in cost based on complexity and capabilities. Simple kits containing only a few files of PHP code can cost anywhere between USD 10 and USD100 to purchase, payable in cryptocurrency or similar means. More complex kits may cost hundreds of dollars. These commonly require backend databases, integrate third-party APIs, have built in "anti bot" or evasion techniques, or even use a basic form of digital-rights management.

During the past quarter, ZeroFox Threat Research has observed several new phishing kit variants produced from popular phishing-kit-as-a-service providers targeting various brands.²⁰ Such kits are offered by private online stores, where threat actors purchase and register their

²⁰ <https://www.zerofox.com/blog/16shop-cash-app-phishing-kit/>

active deployments. Figure 6 is a screenshot of a private store selling phishing kits that target multiple brands and platforms.

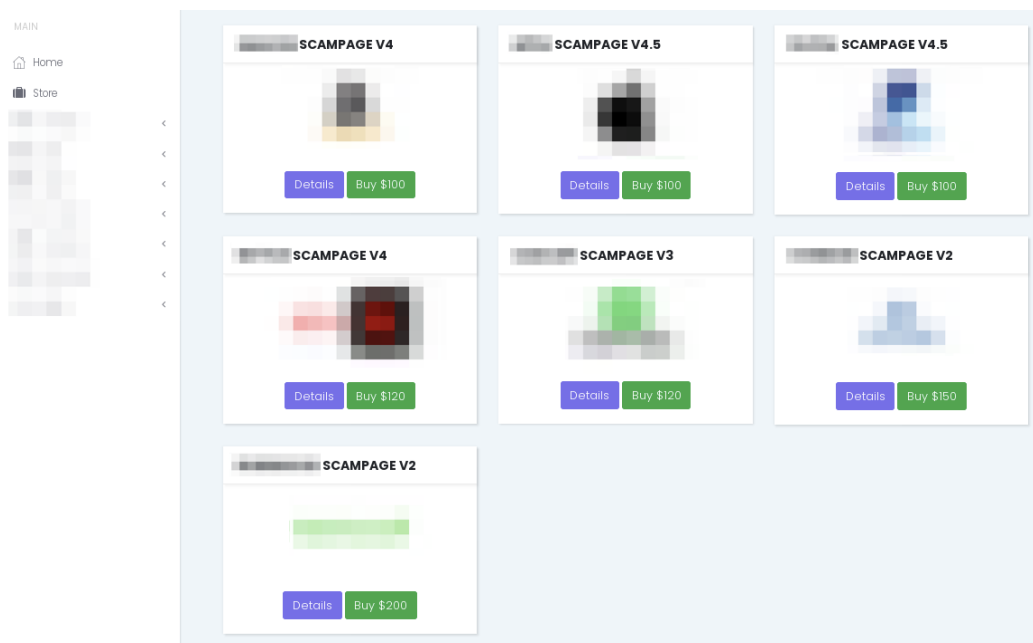


Figure 6: Private online store offering phishing kits targeting multiple brands and platforms

Source: ZeroFox Threat Research

Lure Distribution Mechanisms

A well-known and increasingly popular distribution method for phishing campaigns is via SMS, also referred to as smishing, where lures are sent en masse to large amounts of mobile numbers. Within covert channels, threat actors or groups sell services dedicated to sending massive amounts of SMS messages. Specialized equipment and software are used to facilitate this activity, which is difficult to proactively prevent, as International Mobile Equipment Identity (IMEI) and mobile numbers can be spoofed and changed at random. Figure 7 displays an advertisement for a GSM modem, a device that uses mobile phone technology to provide a data link to a remote network, and an advertisement discussing the cost to send SMS messages for phishing activity.

Other actors will supply lists of "leads" to buyers. These are files containing an agreed number of mobile phone numbers that have been confirmed to be genuine and in use via Home Location Register (HLR) checks, a database containing up-to-date information for every mobile phone subscriber worldwide. An HLR lookup can verify if a mobile phone number is active, switched on, and to which network that number has been assigned.

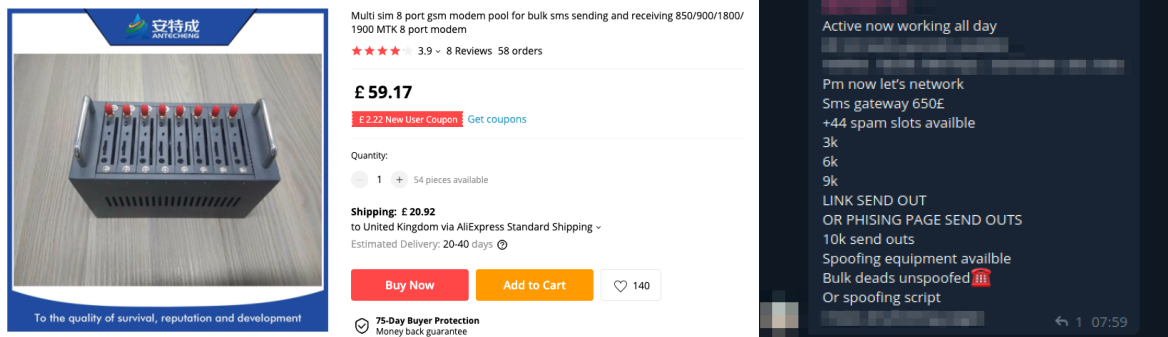


Figure 7: GSM modem used for sending SMS spam (left); message advertising costs of sending SMS messages for phishing (right)

Source: ZeroFox Threat Research

Third-Party Services and APIs

Adoption of third-party services to aid in evading detection has continued to increase this quarter, as more phishing kits are being analyzed to show the utilization of external API providers. Within the space, there are multiple providers of "anti bot" services, which may appear legitimate but are designed to be explicitly used by phishing kits to improve evasive capabilities. Figure 8 displays an example of a popular anti-bot service, along with an open directory containing integrations with popular phishing kits.

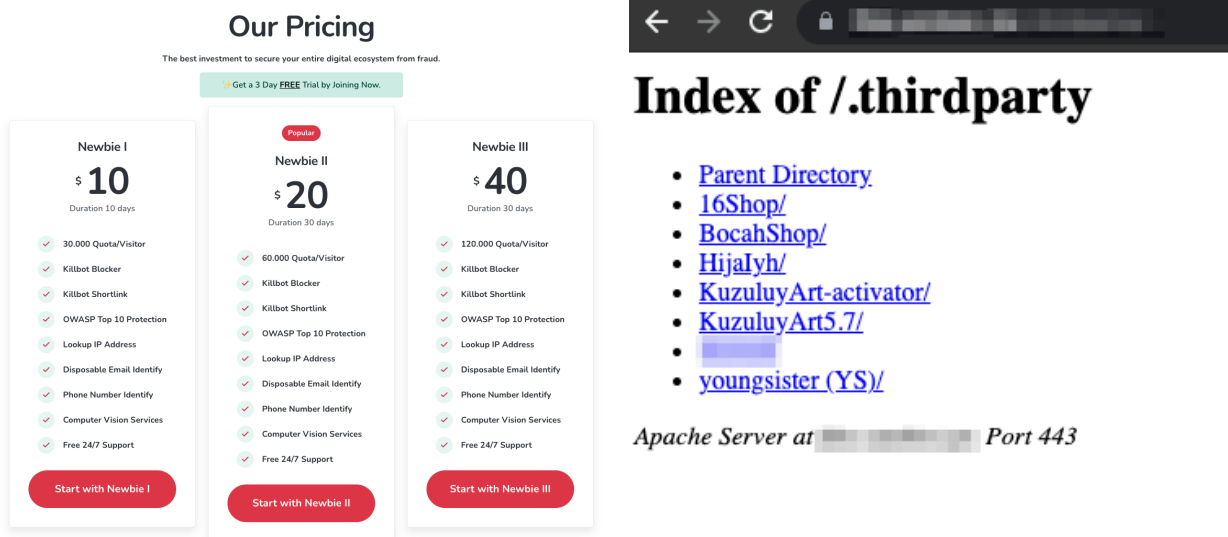


Figure 8: Pricing of a popular anti-bot service commonly integrated with phishing kits (left); an exposed directory of one of these services hosts code that allows direct integration with popular phishing kits (right)

Source: ZeroFox Threat Research

These services are advertised as a tool to block unwanted visitors or "bots" from accessing the customer's website and. These services block or allow access based on the visitor's IP, ISP, geographical location, or browser's user agent. This is also used to prevent access to other services that crawl the web to analyze content for malicious activity.

Retail-targeted Phishing

Depending on the threat actor's appetite for risk, targeting customers of online marketplaces or stores means victims' credentials can be used to quickly cash out with high-value tech purchases or gift cards. There is also an increasing demand for compromised accounts for fast food restaurants and grocery stores that allow purchasing of items online or via mobile apps (Figure 9).

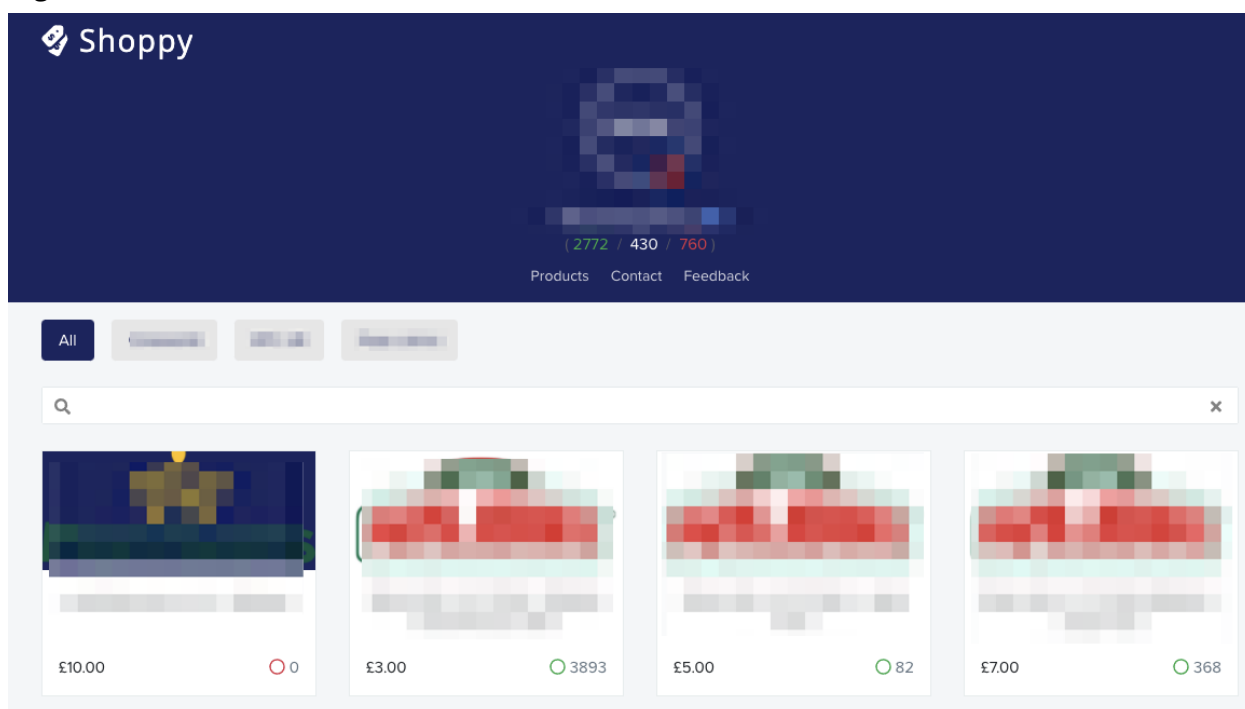


Figure 9: Online storefront selling access to accounts, points, and "methods" for popular grocery and fast food restaurants

Source: ZeroFox Threat Research

ZeroFox Threat Research has observed multiple threat actors selling access to compromised accounts for food and grocery outlets, along with "methods" instructing buyers how to use the credentials in such a way to avoid suspicion and having their orders cancelled. For customers of these threat actors, a small cost of a few dollars can be converted into anywhere up to USD 100 of food with minimal risk.

Finance-targeted Phishing

With the increased vigilance of anti-fraud checks from both banks and online vendors, threat actors have also adapted their techniques and tools to extract more sensitive information from victims to facilitate bypassing "know your customer" (KYC) checks. Many of the latest phishing kits now include additional stages in the victim workflow to prompt the victim to provide identity documentation. Requested information can range from a single "selfie" photo to photos of passports or driver's licenses, which, in combination with other victim data, can be used for fraudulent purposes.²¹ Figure 10 displays an example of this technology on a phishing page fraudulently impersonating a financial services company.

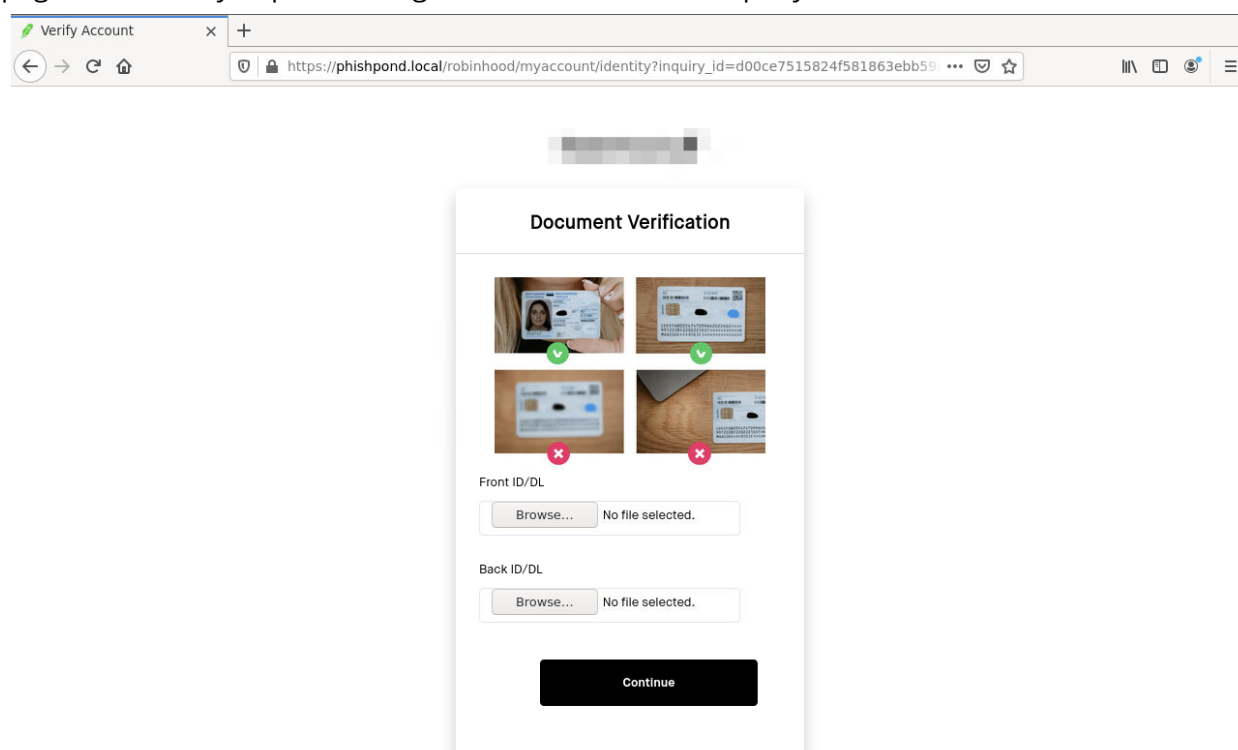


Figure 10: Phishing page requesting the user to upload identity documents

Source: ZeroFox Threat Research

Selling Victim Data

Collected data is commonly sold in the form of "fullz," meaning full credential and/or credit card information has been obtained from the victim. The method of selling can vary depending on the capabilities of the actor but is generally done either in bulk for a set cost or on a per-account basis, with cost varying based on the value or assets of the compromised account (Figure 11). This is standard for accounts with access to monetary funds such as banks. Sellers

²¹ <https://www.zerofox.com/blog/cares-act-fraud/>

may also agree to sell access at a reduced cost in exchange for a percentage of the returns the purchaser makes from "cashing out" the account.

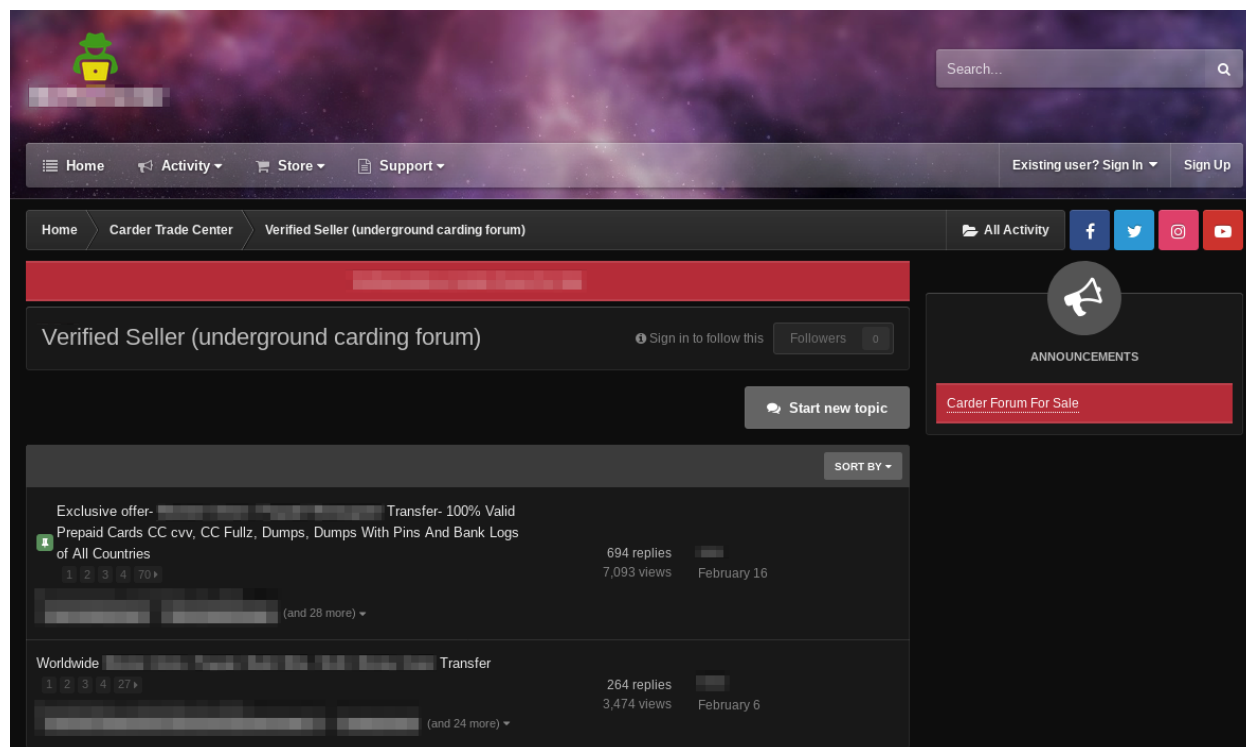


Figure 11: Forum dedicated to selling and sharing of victim data and credit card information sourced from phishing attacks

Source: ZeroFox Threat Research

Top Vulnerabilities and Exploits of Q2 2021

Vulnerability

This quarter, ZeroFox Threat Research tracked vulnerability chatter across social media platforms, cyber criminal underground networks, and covert communication channels to better understand the significance of sharing vulnerability data between researchers and threat actors. From April 1, 2021, to June 30, 2021, on Twitter, there were approximately 119,422 unique common vulnerabilities and exposure (CVE) references across 10,920 vulnerabilities. Many of these vulnerability mentions are automated and track various CVE sources for newly assigned vulnerabilities, like MITRE's @CVEnew account. Most of these mentions are from the security research community, as well as news sources. Figure 12 shows the Top 10 most-discussed CVEs in this timeframe, while Figure 13 highlights the normalized volume of the same CVEs on a weekly basis captured by ZeroFox Threat Research this quarter.

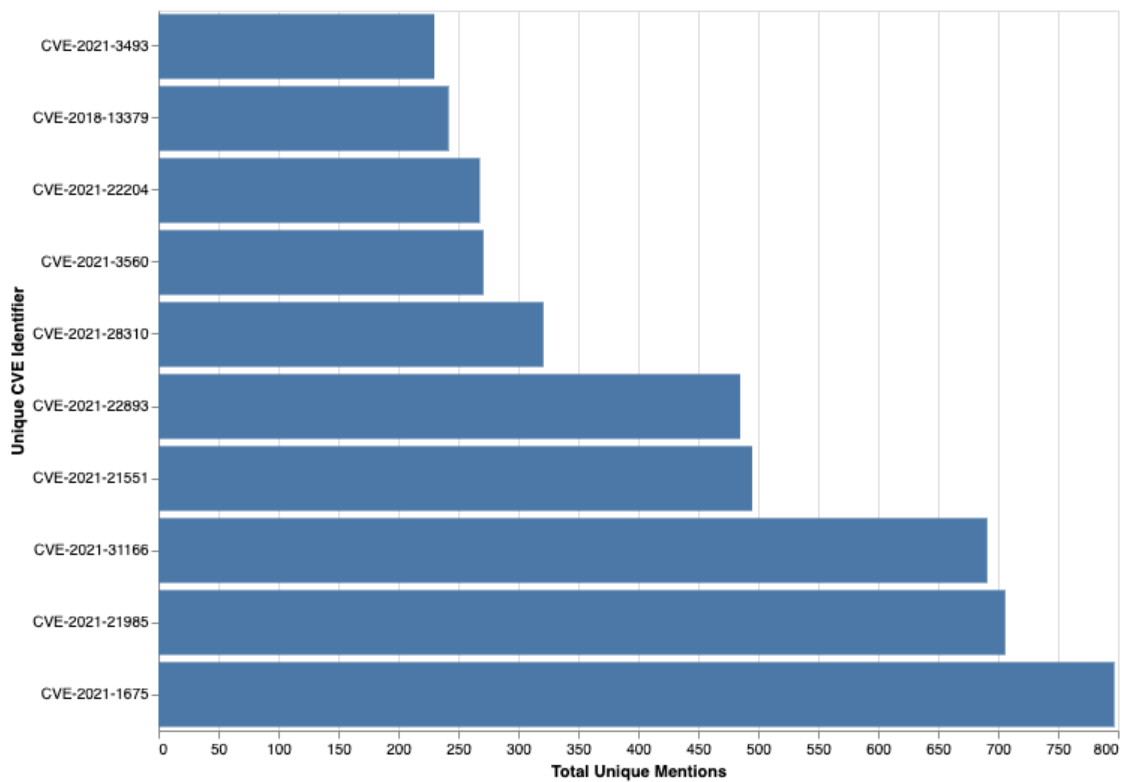


Figure 12: Top 10 CVEs talked about on social media
Source: ZeroFox Threat Research

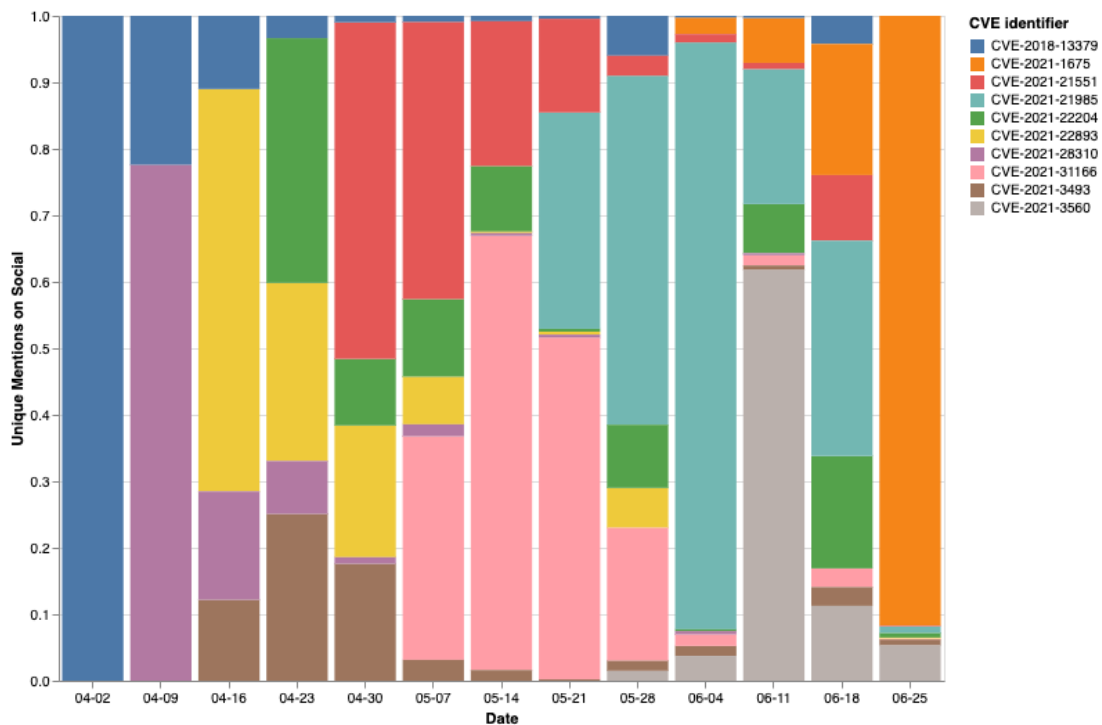


Figure 13: Top 10 CVEs, normalized by volume, throughout each week of the quarter
Source: ZeroFox Threat Research

Figure 13 shows an interesting trend regarding the dominance of the Top 10 vulnerabilities in social media conversations as the disclosure, patch, and news cycles progress week by week. For example, the week of April 2, 2021, is the only week this quarter when a Top 10 vulnerability (CVE-2018-13379) accounted for 100 percent of the conversation. CVE-2018-13379 was a Path Traversal vulnerability that affected FortiOS in Fortigate VPN Servers.²² In that same week, Kaspersky published a blog detailing threat actors who exploited a number of Fortigate VPN Servers and then deployed the Cring ransomware strain on victims. Two weeks later, the US government released an advisory detailing the use of this vulnerability by the Russian Foreign Intelligence Service, or APT 29, to break into systems.²³ To show the efficacy of the news cycle surrounding vulnerabilities, ZeroFox Threat Research plotted each top vulnerability in Figure 14 with information on the week it "dominated" the conversation. The table also specifies the platform, actor information, and the subsequent vulnerability that dethroned the current vulnerability.

Starting Week	Platform	Vulnerability Designation	Date of Release	Threat Actor Association	Dethroned by
04/02/2021	Fortigate VPN	CVE-2018-13379	06/04/2019	APT 29, Cring ransomware	CVE-2021-28310
04/09/2021	Microsoft Desktop Manager	CVE-2021-28310	04/13/2021	Bitter APT	CVE-2021-22893
04/16/2021	Pulse Connect Secure	CVE-2021-22893	04/23/2021	HIDDEN COBRA/North Korea ²⁴	CVE-2021-22204
04/23/2021	Exiftool	CVE-2021-22204	04/23/2021	N/A	CVE-2021-21551
04/30/2021	Dell Client Platform	CVE-2021-21551	05/04/2021	N/A	CVE-2021-31166
05/14/2021	Windows Operating System	CVE-2021-31166	05/11/2021	N/A	CVE-2021-21985
05/28/2021	VMware vSphere	CVE-2021-21985	05/26/2021	N/A	CVE-2021-3560

²²<https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/>

²³ <https://www.ic3.gov/Media/News/2021/210402.pdf>

²⁴<https://www.cpomagazine.com/cyber-security/north-korea-hackers-breached-souths-atomic-energy-research-institute-using-a-vpn-vulnerability/>

06/11/2021	Red Hat Enterprise Linux	CVE-2021-3560	06/03/2021	N/A	CVE-2021-21985
06/18/2021	VMware vSphere	CVE-2021-21985	05/26/2021	N/A	CVE-2021-1675

Figure 14: Table of vulnerability chatter dominance on social media by week in Q2 2021

Source: ZeroFox Threat Research

At the time of this publication, CVE-2018-13379, CVE-28310, and CVE-2021-22893 were the only three vulnerabilities in the Top 10 most-engaged vulnerabilities that had reported actor usage. When searching for news related to these vulnerabilities, most of the research reported discussed the use of these vulnerabilities in a real-world attack. Every single vulnerability afterward did not have in-the-wild exploitation, but most of the news stories, blog posts, and code sharing repositories shared scanning scripts and proof-of-concept (PoC) exploit code.

CVE-2021-1675: A Case of Earnest Misinformation

CVE-2021-1675, or "PrintNightmare" at the time, was published on June 8, 2021. CVE-2021-1675 is a Windows Print Spooler Remote Code Execution (RCE) vulnerability that allows privilege elevation if an attacker has local access to the victim machine, either through hands-on-keyboard, SSH, or having a victim trigger the vulnerability. The vulnerability overtook 90 percent of the unique mentions from Figure 13 by the week of June 25, 2021.

Although CVE-2021-1675 was assigned to the correct vulnerability, a deep-dive analysis of the vulnerability revealed that it was not correctly identified and fixed and that many researchers achieved network-based pre-authentication RCE with the print spooler service.²⁵ Microsoft acknowledged this as a separate vulnerability and subsequently assigned CVE-2021-34527 on July 1, 2021, correctly attributing it to "PrintNightmare."²⁶

Thirty-one GitHub repositories were created from June 5, 2021, to July 1, 2021, for PoCs and scanners for CVE-2021-1675, showing the security research community's commitment to publishing code that takes advantage of the vulnerability in different aspects.²⁷ Many of these PoCs were useful for the community to discuss the implications, but they were also being discussed openly in the cyber criminal underground. For example, two threads on popular

²⁵ <https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/>

²⁶ <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

²⁷ <https://github.com/search?q=CVE-2021-1675+created%3A%3E%3D2021-06-05+created%3A%3C%3D2021-07-01&type=Repositories&ref=advsearch&l=&l=>

cyber crime forums Exploit and XSS showed how criminals can take advantage of the security research community, as seen in Figures 15 and 16.

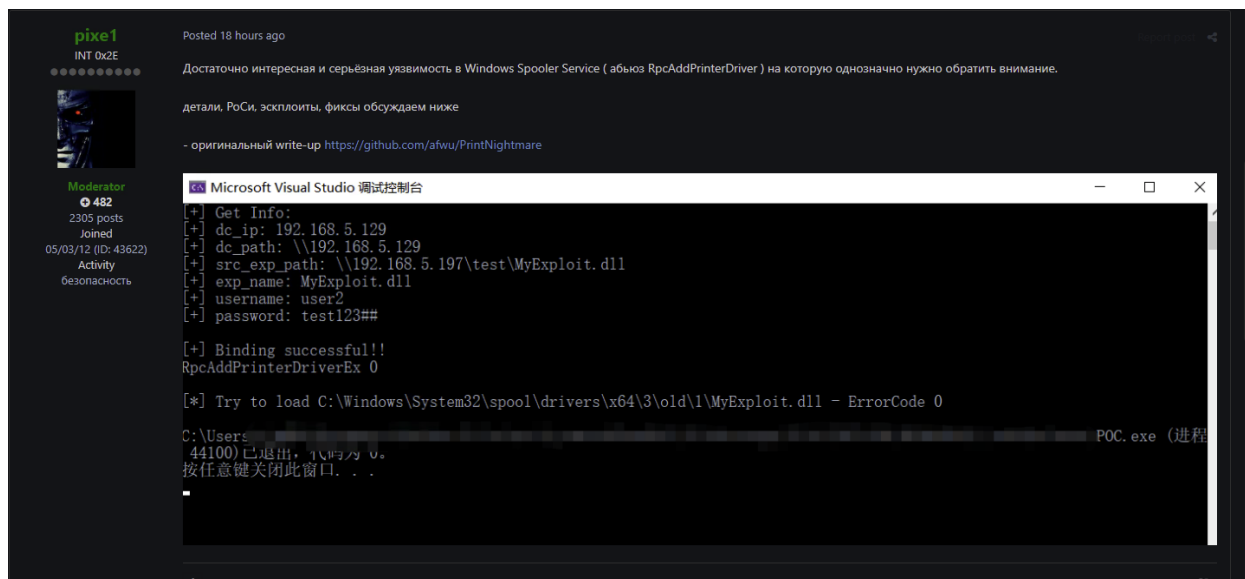


Figure 15: Moderator on Exploit links public PoC for PrintNightmare (CVE-2021-1675)

Source: ZeroFox Threat Research



Figure 16: Member on Bugtraq forum on XSS shares Python PoC code

Source: ZeroFox Threat Research

The misinformation surrounding PrintNightmare and the rush to publish working PoC code influenced threat actors on these forums to discuss the details of CVE-2021-1675. This discourse demonstrated that threat actors rely heavily on the security research community for

information and frequently post PoC details on their forums to share knowledge with each other. (**ZeroFox Note:** On July 15, 2021, Microsoft issued a CVE for a related elevation of privilege vulnerability in the Windows Print Spooler, CVE-2021-34481. As of that date, no patch was issued, and, instead, a temporary fix was recommended.²⁸)

CVE-2021-21985: Vulnerable vCenter Services Offer Foothold Into Organizations

On May 25, 2021, VMware addressed a critical vulnerability, known as CVE-2021-21985, in the vCenter Server application. It is a remote code execution (RCE) in vSphere Client (HTML5) that exists due to a lack of input validation in the Virtual SAN (vSAN) and affects vCenter Server versions 7.0, 6.7, and 6.5. VMware vCenter server is a centralized management application that manages virtual machines and ESXi hosts centrally and is widely used by many companies to manage their infrastructure. Most of these servers reside in large data centers that host terabytes of sensitive data. vSphere Client again is used to access vCenter Server and ultimately manage ESXi servers. The VMware vSAN Health Check plug-in is enabled by default in the vCenter Server that allows an attacker to trigger the attack.

According to Shodan, there are 5,507 instances of public-facing vCenter Servers (Figure 17), with the majority of these running on versions 6.7.0, 6.5.0, and 7.0.x over port 443 (Figure 18). Security researchers found that more than 4,000 vCenter Server instances are still vulnerable to exploitation based on their self-reported versions.²⁹ An attacker with network access to the server over port 443 (HTTPS) can exploit this flaw without authentication to execute commands with unrestricted privileges on the operating system that hosts the vulnerable vCenter Server versions.

²⁸ <https://www.zdnet.com/article/windows-print-spooler-hit-with-local-privilege-escalation-vulnerability/>

²⁹ <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/thousands-of-vulnerable-vmware-vcenter-servers-still-publicly-exposed-cve-2021-21985-cve-2021-21986/>

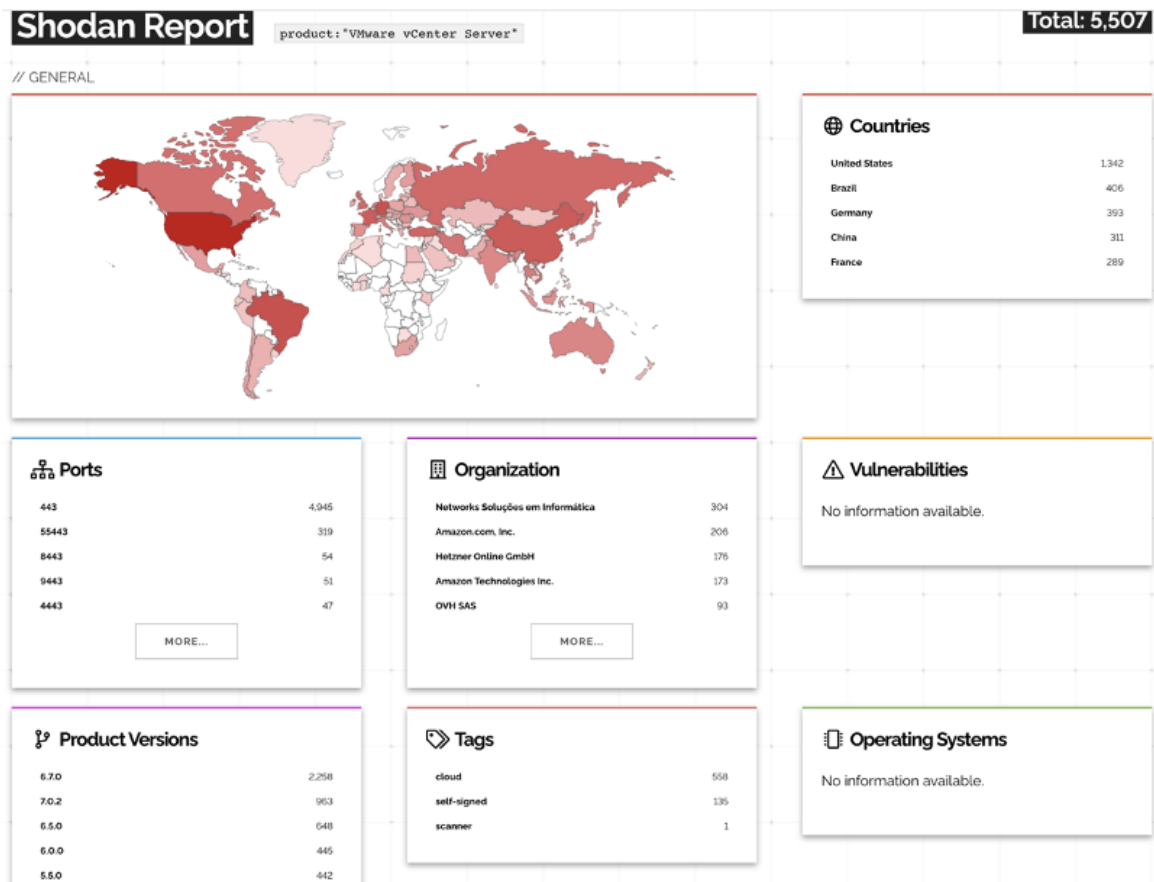


Figure 17: Shodan results showing Internet-facing VMware vCenter Servers

Source: ZeroFox Threat Research

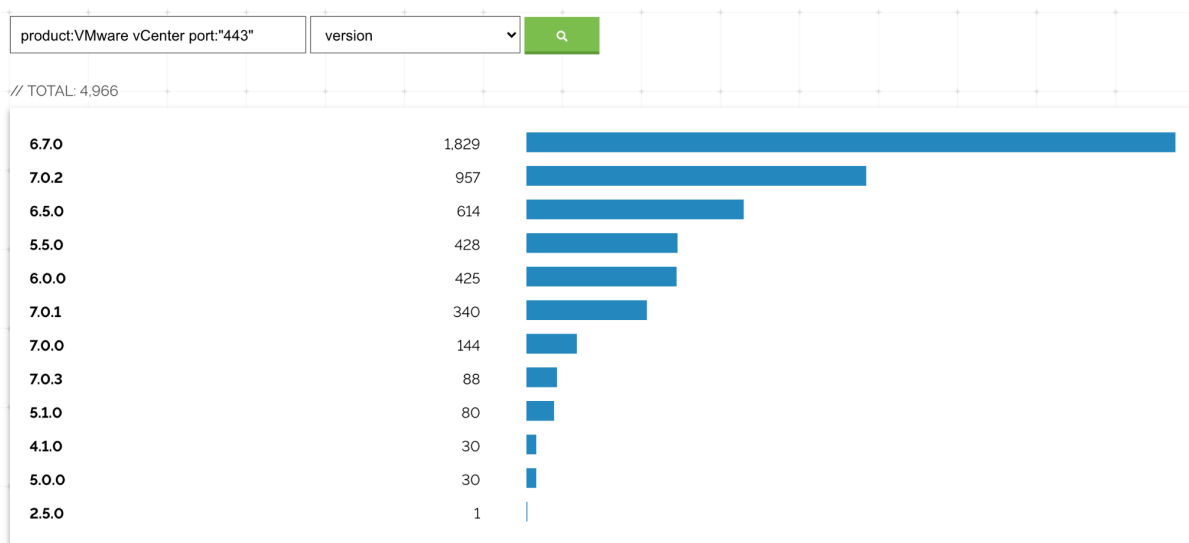


Figure 18: Shodan results of VMware vCenter Server versions on port 443

Source: ZeroFox Threat Research

After the vendor released the patches, several PoC exploits were developed and made publicly available. Researchers detected suspicious activities from external sources attempting to exploit the RCE vulnerability for CVE-2021-21985. Social media trends and chatter reveal that, after the publication of exploit codes, mass Internet scans were discovered where attackers and defenders searched for vulnerable servers (Figure 19). Although there is no evidence of active exploitation, unpatched systems remain an attractive target, and attackers can exploit this vulnerability to take control of the infrastructure.

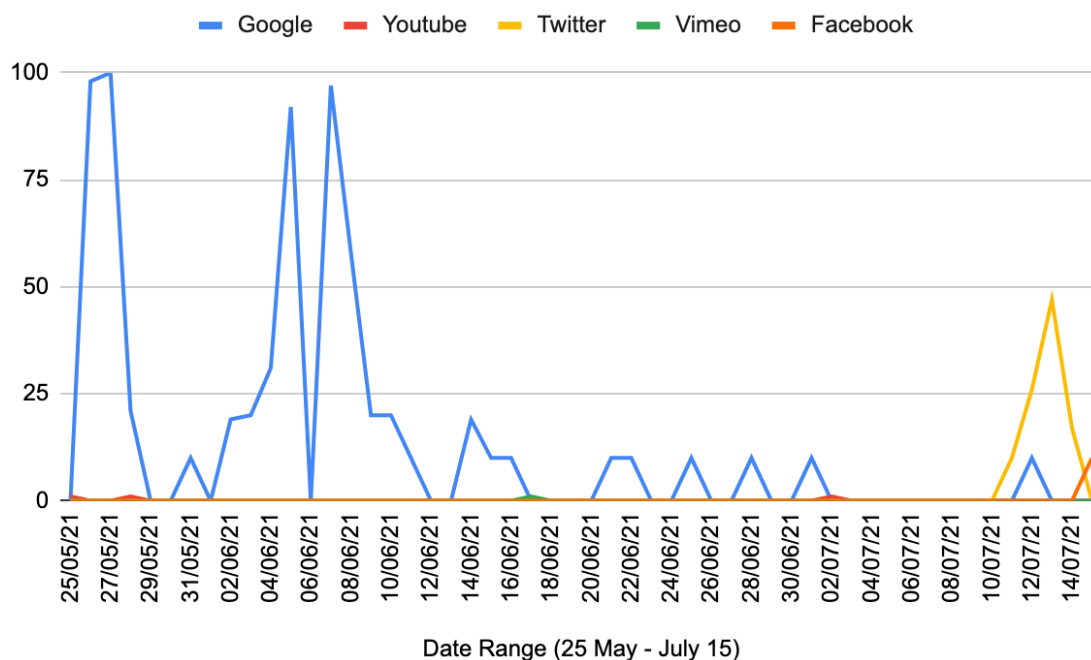


Figure 19: Social media trends for CVE-2021-21985

Source: ZeroFox Threat Research

CVE-2021-31166 - Wormable RCE in Windows HTTP Stack

In the May 2021 Patch Tuesday security release, Microsoft addressed the HTTP Protocol Stack Remote Code Execution vulnerability, tracked as CVE-2021-31166.³⁰ This vulnerability is categorized as highly critical since it is a wormable remote code execution vulnerability and can spread between vulnerable systems across the networks without user interaction. Successful exploitation of this vulnerability could lead to service interruptions, high-value accounts take-over, or complete control of the system.

The flaw resides in the HTTP[.]sys library of HTTP Protocol Stack. The HTTP[.]sys utility allows Windows and applications to communicate with other devices. It can be run independently or in

³⁰ <https://msrc.microsoft.com/update-guide/releaseNote/2021-May>

conjunction with Internet Information Services (IIS). It is also used as a protocol listener by the Windows IIS web server for processing HTTP requests. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted packets to a vulnerable server and trigger arbitrary code execution directly in the Windows operating system kernel, leading to denial-of-service conditions or code execution with kernel privileges. The flaw affects different versions of Windows 10, Windows Server 2004, Windows Server 20H2, and Windows servers enabled with Windows Remote Management (WinRM) and Web Services on Devices (WSDAPI), which also use the vulnerable HTTP[.]sys. WinRM is enabled by default on enterprise editions, while home users have to toggle on the WinRM service manually.

A security researcher published a working PoC exploit code that allows crashing an unpatched Windows system running IIS server and even causes Blue Screen of Death (BSOD). The worming capabilities and elevation of privileges are not included in the PoC. Publishing the exploit PoCs can enable adversaries to leverage the security flaw, scan against exposed vulnerable Windows servers, and create their own exploits—potentially allowing remote code execution and the sale of compromised data on cybercriminal underground marketplaces. At the time of writing this report, ZeroFox Threat Research is unaware of any exploits available in the wild.

Recommendations

In light of the ongoing threat of ransomware, data breaches from security vulnerabilities, and other severe types of cyber threats, organizations should continue to take steps to minimize the risk of becoming a victim of a cyber attack.

- Enable two-factor authentication for all of your organizational accounts to help mitigate phishing and credential stuffing attacks.
- Enforce administrative or application control restrictions to prevent unauthorized installation of software or media.
- Ensure antivirus and intrusion detection software is up-to-date with all patches and rule sets.
- Utilize account permissions best practices, such as role-based access control, least privilege, and restricting root/admin permissions.
- Segment critical network resources using zero-trust configurations.
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks.
- Limit file egress by size and type.
- Disable macros whenever possible.
- Avoid opening unsolicited attachments, and never click suspicious links.
- Enforce best practices on passwords, such as complexity, forced expiration, and prohibiting password reuse.

- Do not share passwords, and do not reuse the same password on different websites and applications.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Consider disabling, or at least logging, all network activity outside of normal business hours for most users where possible.

Conclusion

Over another quarter filled with high-profile cyber activity, the global cyber threat landscape once more demonstrates the evolving nature of cybersecurity and cyber threats. As more ransomware attacks take place against organizations and individuals, it becomes critical for governing bodies to establish a response plan to help those who have become victims. The attention from law enforcement and security researchers on underground marketplace networks may push threat actors to use new methods of communication and collaboration to avoid monitoring of their activities. As threat actors get creative with technology and attack vectors, phishing supply chain ecosystems can help business leaders and security teams understand the inner workings of digital fraud threat actors, as well as the importance of securing applications to prevent phishing attacks. Security researchers will continue to disclose new vulnerabilities that directly affect enterprise organizations and their cohorts. However, it is of utmost importance for security teams to patch and update vulnerable systems, as well as to strategize regarding additional ways to defend against such security vulnerabilities. The first half of 2021 proved that taking the minimum amount of recommended security precautions is not enough in today's threat landscape. The second half of 2021 will require defenders to be even more well-equipped to handle the changing landscape.