



Quarterly Threat Landscape Review

Q3, 2021

Table of Contents

Executive Summary	3
Key Points	3
Ransomware and Malware Activity	4
Ransomware Landscape	4
Malware Landscape	6
National and International Cyber Security Initiatives	7
Top Vulnerabilities and Exploits of Q3 2021	8
Microsoft Security in the spotlight this quarter	11
FORCEDENTRY	12
Phishing Overlaps with Physical Theft	13
Background	13
Details	13
Cybercriminal Underground Networks	18
The emergence of the RAMP	18
Personally Identifiable Information Leaks	19
Compromised Credentials	20
Network Access Requests and Sales	20
Data Breaches	21
Recommendations	23
Conclusion	24

Executive Summary

In the third quarter of 2021 (Q3 2021), the global cyber threat landscape changed in a number of significant ways, some of which included: persistent ransomware attacks; numerous disclosed vulnerabilities; and enhanced threat actor tactics, techniques, and procedures (TTPs). Ransomware groups continued launching attacks using new and existing ransomware types, while the involvement of mobile malware and banking trojans in attacks surged this quarter. The persistence and impact of ransomware led to governments around the world working with cybersecurity experts to promote education and response plans for cyber attacks. Newly-disclosed exploits and vulnerabilities emerged this quarter, including various security flaws in enterprise and cloud software, Apple devices, and a surge of vulnerabilities in Microsoft products. Cybercriminal underground networks endured a quarter rife with data leak advertisements, sale of cybercrime tools, and more groups operating ransomware data leak and digital extortion websites – including the discovery of the Colossus ransomware through ZeroFox collection and detection efforts. Furthermore, ZeroFox Threat Research observed a new type of scam and fraud activity where threat actors steal and unlock digital devices using specially-crafted phishing kits which mimic features used to track devices when lost or stolen. In this Quarterly Threat Landscape Review, ZeroFox Threat Research presents an overview of activity and highlights during Q3 2021.

Key Points

- Ransomware operators continued launching attacks on vulnerable targets while also introducing new updates to extortion tactics. Meanwhile, malware threat actors favored mobile malware and banking trojans this quarter and continued leveraging tools like Cobalt Strike in attack chains.
- The United States (US) government continued efforts towards improving national cybersecurity by working with technology enterprises to decrease cyber attacks on critical infrastructure and imposed sanctions on ransomware payments and negotiations.
- Major operating system vendors experienced a high volume of critical vulnerability disclosures this quarter. Microsoft products endured numerous vulnerability disclosures, including Microsoft Azure flaws and ongoing threats around PrintNightmare. Security researchers also disclosed a critical Apple vulnerability, "FORCEDENTRY," related to exploits used by the Pegasus spyware.
- ZeroFox's internal collection and detection efforts saw ransomware-related content in nearly 47% of our priority reporting, with approximately 21% of priority reporting was related to data breaches, such as Epik. A new forum called "RAMP" debuted on the threat landscape this quarter. On the ransomware front, new ransomware groups emerged that take part in digital extortion schemes.

- Threat actors and scammers developed scams mimicking features used to track and locate misplaced digital devices by leveraging special phishing to exfiltrate information from victims to unlock their stolen devices.

Ransomware and Malware Activity



Malware

Ransomware Landscape

Ransomware Trends

The third quarter saw a number of changes on the ransomware front. Some of the major players from past quarters shifted to smaller presences. In other cases, threat actors that had “rebranded” in previous quarters re-established their prominence under their new names.

As seen in Figure 1 below, the Conti ransomware group settled into a smaller percentage of the total number of attacks after being very active in the second quarter. Though Conti was still a significant factor in the landscape, they were overtaken by the LockBit 2.0 group - a rebrand of the original LockBit group. Newcomer BlackMatter displays similarities to the ransomware used by DarkSide, REvil, and LockBit as well. The group referred to as Grief, who appears at seventh on our list of observed attacks, is a rebrand of the DoppelPaymer group. And the Payload.bin group is believed to be a new manifestation of the Babuk ransomware team.

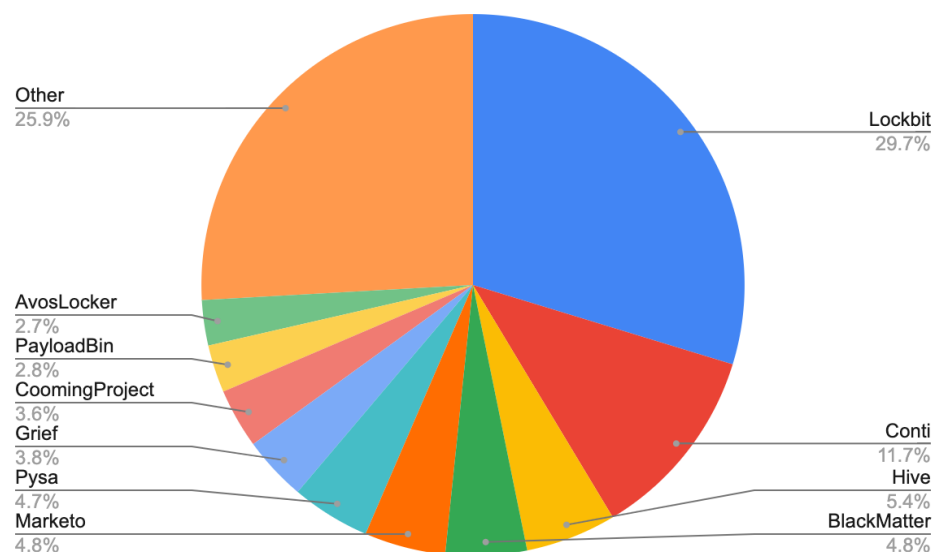


Figure 1. Distribution of Ransomware Attacks and Digital Extortion Observed in Q3 2021

Source: ZeroFox Threat Research

As can be seen in Figure 1, even though the specific groups and their individual percentages have changed, it's continued to be true that approximately 75% of our observed ransomware and digital extortion attacks have been carried out by ten actors, and all other actors combined comprise the other approximately 25% of attacks. Figure 2 and Figure 3, however, indicate a continued upward trend in the number of attacks. This holds true across all of 2021 for average daily attacks, number of attacks month over month, and number of attacks per quarter.

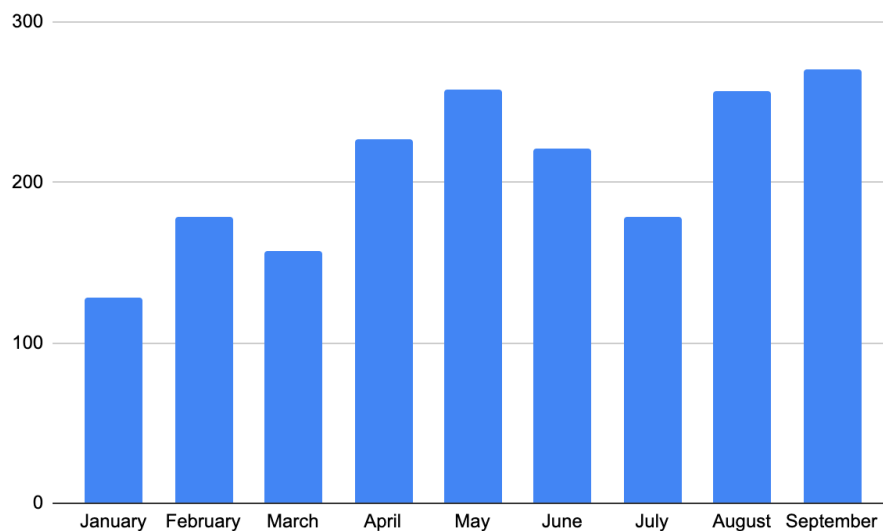


Figure 2. Number of Ransomware Attacks per Month, 2021
Source: ZeroFox Threat Research

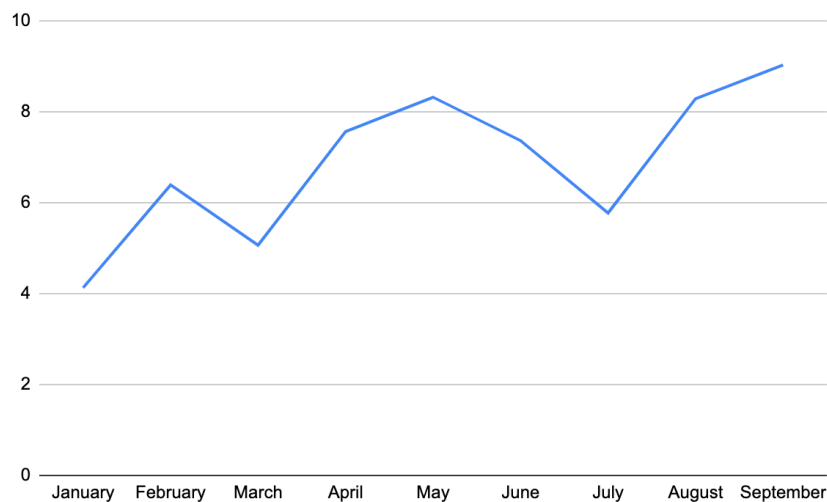


Figure 3. Average Number of Ransomware Attacks per Day by Month, 2021
Source: ZeroFox Threat Research

ZeroFox Research did observe a downward trend in the number of attacks beginning in May 2021 and continuing into July. We believe that this is a result of the law enforcement

crackdowns and high-profile attacks earlier this year. Despite that slowdown and some intervention in the way of government policies and private industry focus, attack groups seem to have regained their motivation and performed attacks in keeping with former growth. Of particular note is LockBit 2.0, which emerged from their rebrand in July 2021 and have since become more prolific than any other group we have observed.

New Ransomware Developments

A number of new developments occurred in Q3 2021, or in some cases found their stride from their emergence late last quarter. The first is the RAMP cybercrime forum, Ransom Anonymous Market Place, which is an online forum dedicated to data leaks and ransom actors. It was launched in July 2021 after a split within the Babuk ransomware group, with the Admin from Babuk forming RAMP and the rest of the group rebranding as Babuk2.0.

There is also news of potentially four new ransomware groups emerging on the scene. The first group, Colossus, was discovered by ZeroFox Research on September 24, 2021, and could possibly be related to EpsilonRed, BlackCocaine, and REvil samples.¹ Similarly, an apparent derivative of Babuk ransomware, dubbed Delta Plus, was detected by ZeroFox on September 28, 2021.²

A group referred to as AtomSilo emerged in September, primarily taking advantage of a vulnerability in Confluence servers to launch their attacks. Also, a group referred to as Spook emerged on the scene in September 2021, and has drawn comparisons that lead some researchers to believe that Spook is a rebrand of the currently inactive Prometheus ransomware group.

Malware Landscape

While ransomware once again dominated the headlines this quarter, a number of significant events have emerged in other components of the malware community, as well.

Mobile malware continues to surge in activity. The latest threat is an attack on Androids called Flubot. Though first observed in December 2020, it has continued to accelerate and evolved in Q3 2021. It is malware with an initial infection vector of a received SMS message, or of masquerading as an update for the phone. Once installed, its purpose is to steal passwords, banking information, and other sensitive data being transmitted by the phone. The malware even has the ability to spread itself to infect other phones.

Banking trojans also spiked in popularity this quarter. Though they are all several years old at this point, versions of Dridex, IcedID, and Qakbot all surged into top spots on the list of most common infections this quarter. All three have contributed significantly to the highest rates of malware infections observed in over two years.

Additionally, we continue to see a rise in the adoption of malware and tools leveraged by multiple threat actors, particularly in multi-component attack chains such as those used in "as a

¹ <https://cloud.zerofox.com/intelligence/advisories/15791>

² <https://cloud.zerofox.com/intelligence/advisories/15829>

service" (aaS) models. After surviving an attempted takedown by Microsoft and other partners, Trickbot rose to one of the highest infection rates among malware. Cobalt Strike, Metasploit, Mimikatz, and PowerShell Empire (and their derivatives, such as Vermilion Strike) continue to dominate the post-exploitation landscape. And frequently combined with these attacks are information stealers such as Raccoon, Redline, and Vidar.³

National and International Cyber Security Initiatives

| Geopolitical & Physical

This quarter, governments worldwide continued prevention efforts for cyberattacks on organizations and individuals. New policies and legislation were drafted in Q3 2021 after large-scale cyber attacks targeted global businesses in 2021, such as the SolarWinds Orion breach, and ransomware attacks on Colonial Pipeline and Kaseya. Due to the impact of cyber attacks on small to large businesses worldwide, governing bodies drafted legislation and initiatives that promote cybersecurity education and programs to help companies prevent and address cyberattacks. Some initiatives in Q3 2021 were demonstrated by countries in Europe.⁴ The United Kingdom (UK) launched a bug bounty program on behalf of the UK Ministry of Defence (MoD) that allowed security researchers to identify vulnerabilities in MoD's digital assets, and apply appropriate patches to the flawed software. France released a "cyberattack alert system" to help inform small- and medium-sized companies of attacks against their organizations and to take appropriate action in response to cyber attacks. Italy introduced a national cybersecurity agency, "Agenzia per la Cybersicurezza Nazionale," that aims to combat cyber attacks targeting Italy, as well as securing cloud infrastructure for the country.

The United States continued efforts to develop strategies for cyber attack prevention, especially as ransomware operators consistently target US-based organizations. In the second quarter of 2021 (Q2 2021), US president Joe Biden's administration published Executive Order 14028, which presents a thorough set of plans to improve the US cyber security posture. The plans in the executive order continued in Q3 2021 when the Biden administration met with major technology companies in an effort to work with the federal government to invest and secure critical infrastructure.⁵ Some of the companies involved with the initiative are Apple, Microsoft, and Google, and promise to improve security features within their products and services. Furthermore, the Administration also directed the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) to develop specifications for managing and securing critical infrastructure.⁶

In addition to ransomware-related prevention efforts, the US Department of the Treasury's Office of Foreign Assets Control drafted sanctions for individuals and organizations who choose

³ <https://cloud.zerofox.com/intelligence/advisories/15712>

⁴ <https://www.csoonline.com/article/3630632/9-notable-government-cybersecurity-initiatives-of-2021.htm>

⁵ <https://techcrunch.com/2021/08/26/big-tech-pledges-billions-to-bolster-u-s-cybersecurity-defenses/>

⁶ <https://www.zdnet.com/article/biden-signs-memo-ordering-cisa-and-nist-to-develop-cybersecurity-performance-goals-for-critical-infrastructure/>

to pay ransom demands using the SUEX cryptocurrency exchange.⁷ The intent of these sanctions is to prevent victims of ransomware attacks from complying with threat actor demands to retrieve stolen information and decryption keys. By participating in ransomware negotiations and payments, threat actors can profit from nefarious activities and continue their operations, leading to more attacks on vulnerable targets.

These initiatives from governing bodies demonstrate the critical need for improving cybersecurity education and response worldwide. As threat actors continue launching attacks on organizations and individuals, world leaders must work with cybersecurity experts to develop solutions that decrease the chances of attacks. Ransomware played a significant role in large-scale attacks in 2021, and operators continue evolving their strategies to ensure targets meet their demands. Only time will tell if such programs and sanctions present an effective solution for cyber attacks.

Top Vulnerabilities and Exploits of Q3 2021

Vulnerability

ZeroFox tracked vulnerability chatter across social media platforms, cybercriminal underground networks, and covert communication channels to better understand the significance of sharing vulnerability data between researchers and threat actors. On Twitter, from July 1, 2021, to September 30, 2021, there were approximately 10,4048 unique mentions of Common Vulnerabilities and Exposure (CVE) references across 11,834 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 4 shows the top 10 most discussed CVEs in this timeframe, while Figure 5 highlights the normalized volume of the same CVEs on a weekly basis captured by ZeroFox Threat Research this quarter.

⁷ <https://home.treasury.gov/news/press-releases/jy0364>

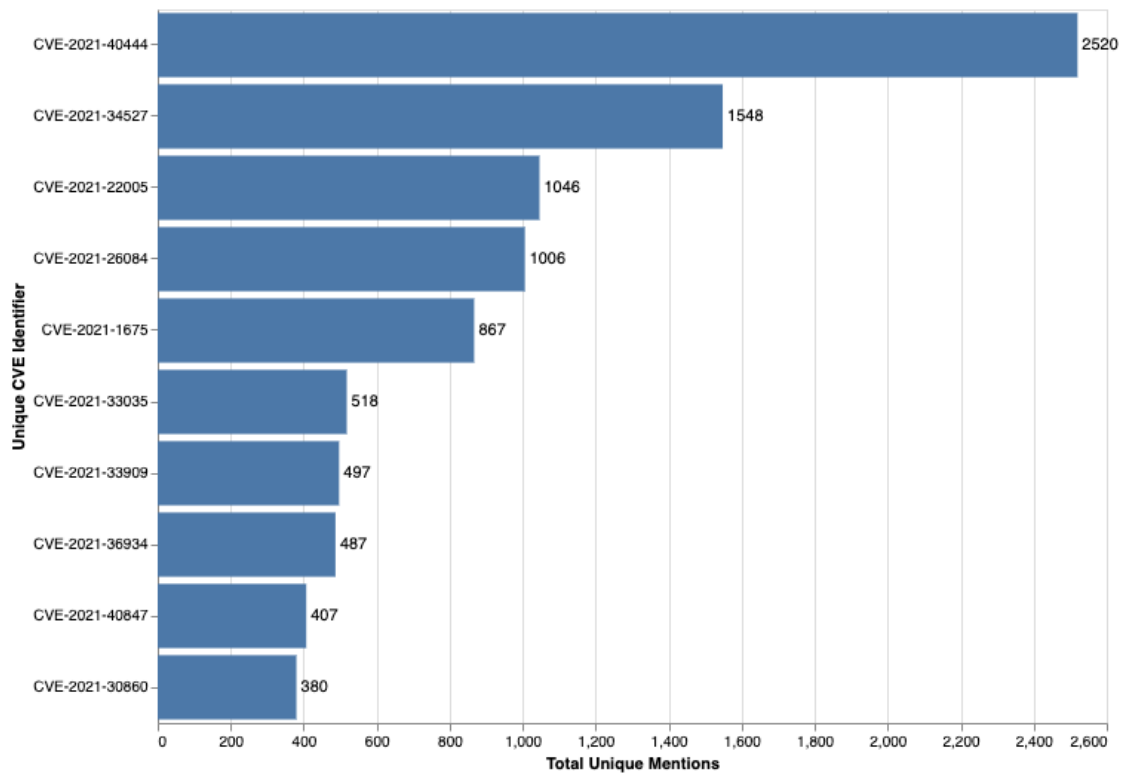


Figure 4. Top 10 CVEs talked about on Social Media
Source: ZeroFox Threat Research

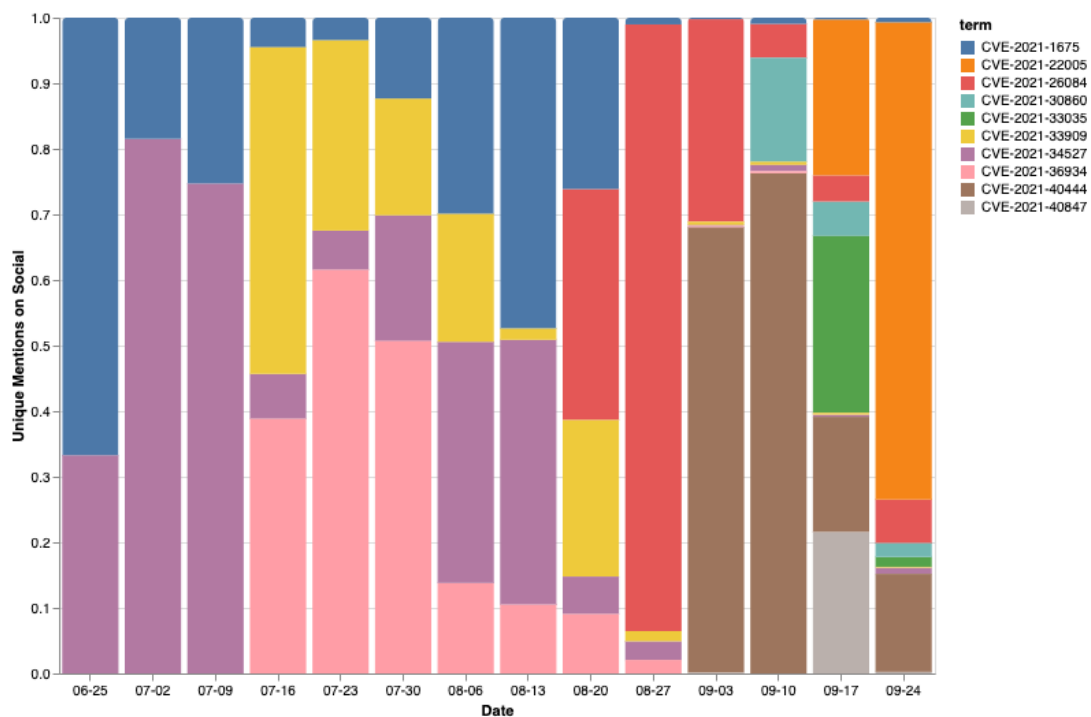


Figure 5: Top 10 CVEs, normalized by volume, throughout each week of the quarter
Source: ZeroFox Threat Research

To show the efficacy of the news cycle surrounding vulnerabilities, ZeroFox Threat Research plotted each top vulnerability in Figure 6 with information on the week it "dominated" the conversation – the time span by which a single vulnerability was discussed more than any other vulnerability. The table also specifies the platform, actor information, and the subsequent vulnerability that dethroned the current vulnerability.

In Q3 2021, Microsoft vulnerabilities overshadowed the information security conversation and news cycle. PrintNightmare, HiveNightmare/SeriousSam, and the MSHTML vulnerability were the most talked about vulnerabilities for 9 out of the 12 weeks in the quarter. ZeroFox Threat Intelligence wrote about PrintNightmare in the Q2 2021 Quarterly Threat Landscape Review. The primary concern at the time was that there was misattribution surrounding the vulnerability, as the flaw resembled another print spooler service vulnerability. PrintNightmare now refers to a group of vulnerabilities, CVE-2021-1675, CVE-2021-34527, and CVE-2021-36958.

Besides the additional two vulnerabilities being added to the PrintNightmare arsenal, one other possible explanation for the sustained coverage is how quickly ransomware groups weaponized PrintNightmare. Two such examples of PrintNightmare vulnerabilities being used in the wild occurred when the Vice Society and Magniber ransomware groups used one or more PrintNightmare vulnerabilities against a victim.⁸ There was a separate instance of Conti acknowledging the use of PrintNightmare, according to their leaked playbook.⁹

Week Start	Platform	Vulnerability Designation	Alternate Name	Release Date	Actor Association Examples	Dethroned by
06/25/2021	Microsoft Windows	CVE-2021-1675	PrintNightmare	06/08/2019	APT29 Magniber Vice Society	CVE-2021-34527
07/02/2021	Microsoft Windows	CVE-2021-34527	PrintNightmare	07/01/2021	Magniber	CVE-2021-33909
07/09/2021	Linux Kernel	CVE-2021-33909	Sequoia	07/09/2021	N/A	CVE-2021-36934
07/16/2021	Microsoft Windows	CVE-2021-36934	HiveNightmare; SeriousSAM	07/20/2021	APT32	CVE-2021-34527
08/06/2021	Microsoft Windows	CVE-2021-34527	PrintNightmare	07/01/2021	Magniber	CVE-2021-1675
08/13/2021	Microsoft Windows	CVE-2021-34527	PrintNightmare	07/01/2021	Magniber	CVE-2021-26084
08/20/2021	Confluence Server & Data Center	CVE-2021-26084	N/A	08/25/2021	TeamTNT	CVE-2021-40444

⁸ <https://cloud.zerofox.com/intelligence/advisories/15667>

⁹ <https://www.bleepingcomputer.com/news/security/translated-conti-ransomware-playbook-gives-insight-into-at-tacks/>

09/03/2021	Microsoft Windows	CVE-2021-40444	N/A	09/07/2021	Ryuk	CVE-2021-33035
09/17/2021	Apache Open Office	CVE-2021-33035	N/A	09/23/2021	N/A	CVE-2021-22005
09/24/2021	VMWare VCenter Server	CVE-2021-22005	N/A	09/21/2021	N/A	N/A

Figure 6. Vulnerability Chatter Engagement Dominance on Social Media by Week in Q3 2021

Source: ZeroFox Threat Research

Microsoft Security in the spotlight this quarter

This quarter was particularly fruitful for vulnerabilities, attack techniques, and general discovery of attacks for Microsoft products. Although Microsoft Windows was the primary technology being highlighted by CVEs, there were numerous Azure vulnerabilities and a new Windows Attack Technique that was also newsworthy. These Azure vulnerabilities and attack techniques do not have specific designations and Microsoft seemed to struggle with a standard response for these vulnerabilities to their customer base.

PetitPotam

In July 2021, a security researcher discovered an attack method known as PetitPotam, which can be used to abuse the authentication protocol NTLM, developed by Microsoft.¹⁰ An attacker can hijack the authentication session by establishing a connection to the server with the help of Microsoft's Encrypting File System Remote Protocol (MS-EFSRPC), which in turn allows them to manipulate the configuration and make the server believe that it has permitted access to legitimate users.¹¹ An attacker must be inside the network and have valid credentials (non-privileged) to perform the attack. The most common way of achieving it is via phishing attacks. The LockFile ransomware operators implemented PetitPotam exploits in attacks, which used a technique known as intermittent encryption to evade detection. Microsoft has issued patches in its August 2021 update to address this vulnerability.

ChaosDB: Azure Cosmos DB Vulnerability

An Israeli-based cybersecurity firm discovered a vulnerability in Microsoft's proprietary Azure Cosmos DB, a globally distributed and managed NoSQL database service. The flaw allows threat actors secure and unrestricted access to accounts and databases affecting Microsoft Azure customers. This security flaw, named ChaosDB, was exploited for several months before its discovery.¹² In 2019, Microsoft added a new add-on package that allowed Cosmos DB to leverage capabilities in Jupyter Notebooks, which Microsoft enabled by default in February 2021. A misconfiguration in Notebooks leads to possible elevation of privileges allowing full read, write, and delete permissions on the databases. Microsoft required Azure customers and

¹⁰<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

¹¹ <https://msrc.microsoft.com/update-guide/vulnerability/ADV210003>

¹² <https://chaosdb.wiz.io/>

network administrators to take appropriate steps to protect their Cosmos databases, including generating new digital keys used to securely access such systems.

OMIGOD Vulnerability Affecting Azure

A critical remote code execution (RCE) vulnerability, named OMIGOD (CVE-2021-38647), was discovered affecting the Microsoft Azure agent for Linux installed and configured with Open Management Infrastructure (OMI) versions before 1.6.8.¹³ When a user configures a Linux virtual machine (VM) in Microsoft's Azure, the OMI component gets installed with root privilege by default, which enables services like Azure Automation Accounts, Update Management, Log Analytics, and Configuration Management. When the OMI agent is configured for remote management, it runs on HTTP/s typically on port 5986. Any user with network access can trigger this flag by sending a specially crafted message via HTTPS over a publicly accessible remote management port bypassing the authorization, elevating the privileges to execute Operating System (OS) commands, and executing arbitrary code on the vulnerable Linux VM.

Azure Active Directory Undetected Brute-Force

Security researchers at a US-based cybersecurity firm discovered a vulnerability in a protocol used by the Azure Active Directory Seamless Single Sign-On (SSO) feature. The flaw could allow an attacker to launch a single-factor brute-force attack against Azure Active Directory (AD), suppressing the log-in events in a targeted network.¹⁴ SSO is a standard method of authentication used in Windows networks. Because Azure AD does not log autologons, it gives attackers an advantage to perform brute-force attacks on the endpoints undetected. Attackers can exploit this vulnerability in Seamless SSO and Azure AD, including Pass-through Authentication (PTA).

Microsoft clarified that precautions against brute-force attacks already apply to the endpoints and that the tokens allotted by the UserNameMixed API restrict access to data. Such calls for access tokens are protected by Conditional Access, Azure AD Multi-Factor Authentication, Azure AD Identity Protection, and surfaced in sign-in logs.

FORCEDENTRY

Apart from Microsoft vulnerabilities, Apple devices made headlines when security researchers discovered a critical vulnerability in Apple devices dubbed "FORCEDENTRY," which was associated with a string of zero-day and zero-click exploits targeting Apple devices weaponized by the Pegasus malware. Tracked as CVE-2021-30860, FORCEDENTRY gets its name from the ability to circumvent Apple's BlastDoor security system for iMessage, Apple's instant messaging service. Recent Pegasus attacks revealed that attackers compromised iOS devices through the iMessage application in highly targeted attacks. The exploit itself is delivered via a payload of one or several PDF and PSD files via SMS, which may be obfuscated by changing file extensions to '.gif.' These files are specifically crafted to cause an IMTranscoderAgent crash on the device

¹³ <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647>

¹⁴ <https://arstechnica.com/information-technology/2021/09/new-azure-active-directory-password-brute-forcing-law-has-no-fix/>

via an integer overflow, which leads to arbitrary code execution. This exploit chain was used to deliver Pegasus malware to specific targets.

Phishing Overlaps with Physical Theft



| PII & Fraud



| Brand

Phishing is a well-known type of attack, which consistently proves to be a threat to enterprises and consumers alike. However, there is a niche form of phishing that directly overlaps with criminals and criminal groups involved in physical theft. These phishing attacks assist criminals in profiting from the theft of mobile and technology devices.

Background

During public holidays, it is not uncommon to see an increase in phishing attacks using specialised types of phishing kits and services, targeting retail technology brands. Many thieves who target households and individuals tend to focus on obtaining technology goods with high resale value, and after holidays such as Black Friday or Christmas, many homes have an abundance of new portable devices.

Over the years, many technology hardware companies have developed and provided tools to customers in order to track and lock their portable devices. These controls are designed to be used in case of loss or theft, blocking unauthorised access to the device and providing contact details for the original owner. The locking of a device will also prevent third-parties from performing a factory reset, or wiping the device, in order to resell it.

Details

Once the device is locked, the only way to restore functionality is for the original owner to log in to their account and disable the lock or lost device mode. For an individual that has just obtained or stolen the device, this renders it practically useless.

Since the introduction of these controls however, a specialised type of phishing kit, sometimes referred to as an "unlocker," has appeared on the market. These unlocker kits are directly sold or utilised by criminal groups to unlock stolen goods.

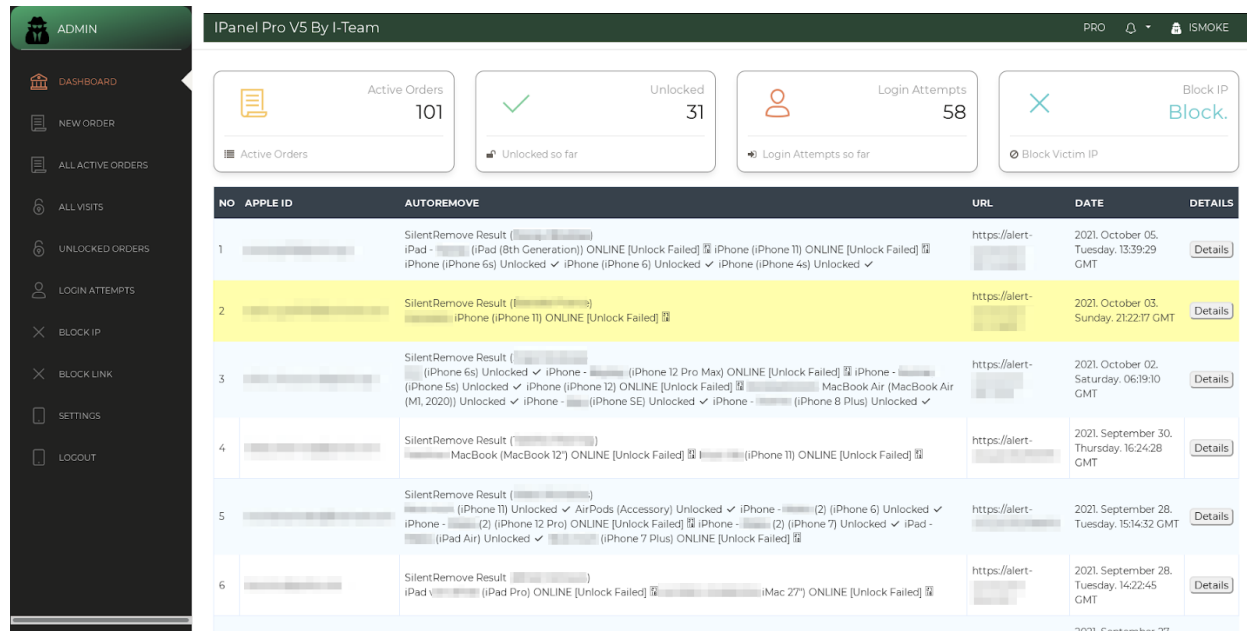


Figure 7. The administrative dashboard of an active unlocker kit, designed to phish victims of theft. This page details recent attacks and their successes.

Source: ZeroFox Threat Research

These types of phishing kits are designed specifically for phishing victims of theft to obtain their account details, in order for the holder of the stolen device to log in, and remove the device lock and tracking before resetting the device back to its original state for resale or use. (**ZeroFox Note:** The "holder" in this context refers to the individual physically holding the device, such as the kit operator, the actor that stole the device, or the actor that bought the stolen device.)

The kits are often sold with licenses, allowing specific individuals to log in to the interface, and orchestrate a phishing attack. When creating these attacks, they are often referred to as "orders." Criminal groups can either use the kit themselves to unlock devices, or oftentimes, they will pay another individual to orchestrate the attack for them.

NO	DEVICE	URL	SCRIPT	AFTER LOGIN	DETAILS	ACTION
1	iPhone 11 Pro Max	https://[REDACTED]/GT-21609	New Dual iCloud/FMI	map	Details	Delete
2	iPhone 11 Pro Max	https://[REDACTED]/GT-19239	New Dual iCloud/FMI	map	Details	Delete
3	iPhone 11 Pro	https://[REDACTED]/GT-16269	Maps Connect	map	Details	Delete
4	iPhone 12 Pro Max	https://[REDACTED]/NT-25881	New Dual iCloud/FMI	map	Details	Delete
5	iPhone 12 Pro Max	https://[REDACTED]/dsfs	New FMI Popup (Custom Map)	map	Details	Delete
6	iPhone 11 Pro Max	https://[REDACTED]/GT-72688	FMI 6 Digits Passcode (Login First)	map	Details	Delete
7	iPhone 12 Pro Max	https://[REDACTED]/L6c29D	New Dual iCloud/FMI	map	Details	Delete
8	iPhone 12 Pro	https://[REDACTED]/GT-79071	New Dual iCloud/FMI	map	Details	Delete
9	iPhone 12	https://[REDACTED]/GT-32767	New Dual iCloud/FMI	map	Details	Delete
10	iPhone 11	https://[REDACTED]/L11c542D	New Dual iCloud/FMI	map	Details	Delete

All Links...

<<<12345678910111213>>>

Figure 8. An active phishing kit listing all active "orders." Some deployments contain details on hundreds of stolen devices.

Source: ZeroFox Threat Research

The proliferation of encrypted messaging platforms in recent years has seen a rapid adoption by individuals who have obtained stolen goods, and are looking for services to unlock them. Many channels exist purely to advertise such services, with users vouching for each other and reporting successfully unlocked devices.

These services do not only extend to mobile phones either, with specialist kits also existing for unlocking laptops, tablets, smart watches, and desktop computers.

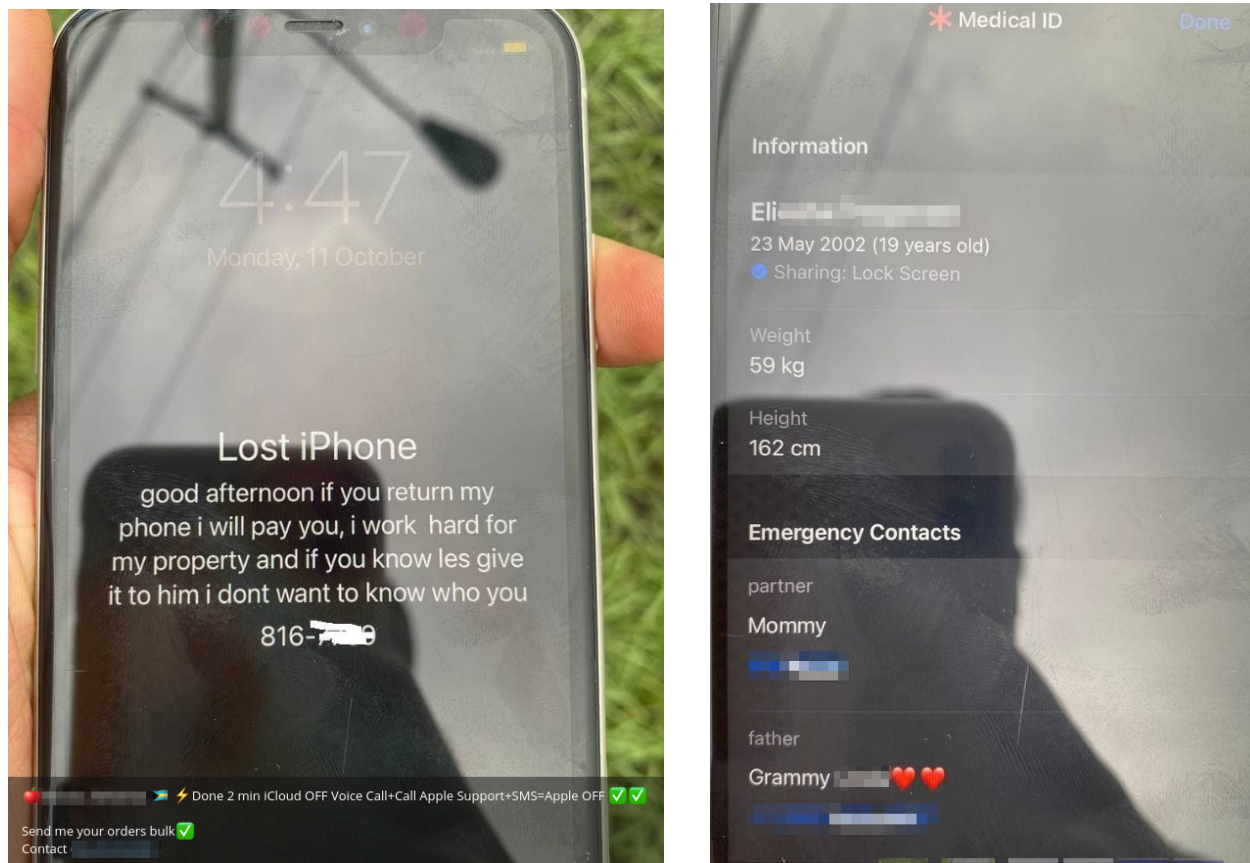


Figure 9. A stolen device listing contact information of the owner (Left). The medical ID information stored on the device, often used to aid in the phishing attack (Right).

Source: ZeroFox Threat Research

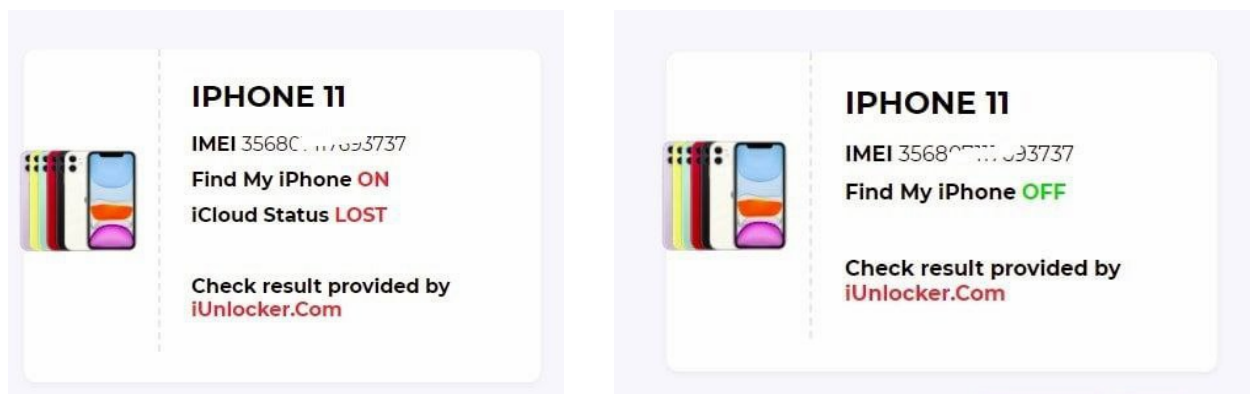


Figure 10. Follow up messages sent to the channel, confirming the successful unlock of the device.

Source: ZeroFox Threat Research

The phishing attack itself is a fairly standard operation, in that it is designed to obtain credentials from the victim. The sophistication and preparation of the attack comes from creating the targeted lure and the design of the victim workflow. Lures are often sent via SMS,

as contact numbers are typically provided on either the locked devices screen or emergency contact details. The lures inform the recipient that their device (including the device's name/model) has been located, and they can log in to their account to see its current location. If instead an email address is listed as contact information, a lure in the form of an email or iMessage is sent to the victim.

Once the victim has clicked the specially crafted link within the lure and landed on the phishing page, the victim workflow begins. These are highly configurable and replicate the genuine interaction steps completely.

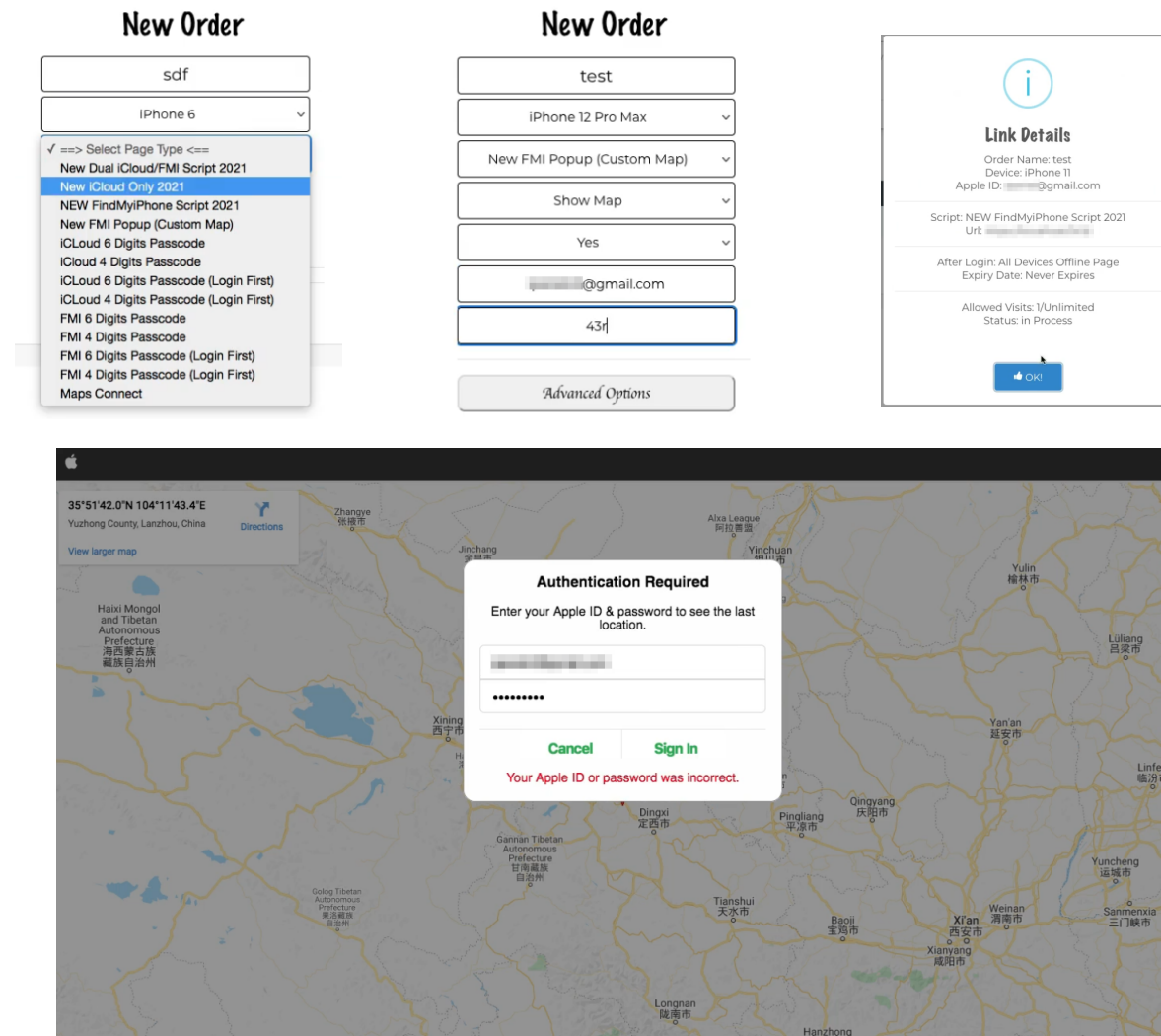


Figure 11. Configurable options for the phishing attack (Top). One of the many possible phishing pages victims can be presented with (Bottom).

Source: ZeroFox Threat Research

Once the attacker has gained access to the account, they quickly disable any "find my device" services, and unlock, or mark, the device as found. Within minutes, the holder of the stolen device can perform a factory reset and remove any association with the previous owner.

Such devices are then set up "as new," and either used by the holder of the stolen device, or sold via online marketplaces.

Cybercriminal Underground Networks



I Deep Dark Web & Criminal Underground

As part of our regular threat intelligence collection efforts, ZeroFox has investigated numerous events collected from cybercriminal underground forums this quarter based on ZeroFox global standing intelligence requirements. At nearly 47% of these observed events, ransomware accounted for a large portion of the activity. Data breaches and network access activity, which can also tie into ransomware, accounted for 21.2% and 19.8% of observed activity, respectively. Malware trailed behind at just 5.1% of observed activity this quarter.

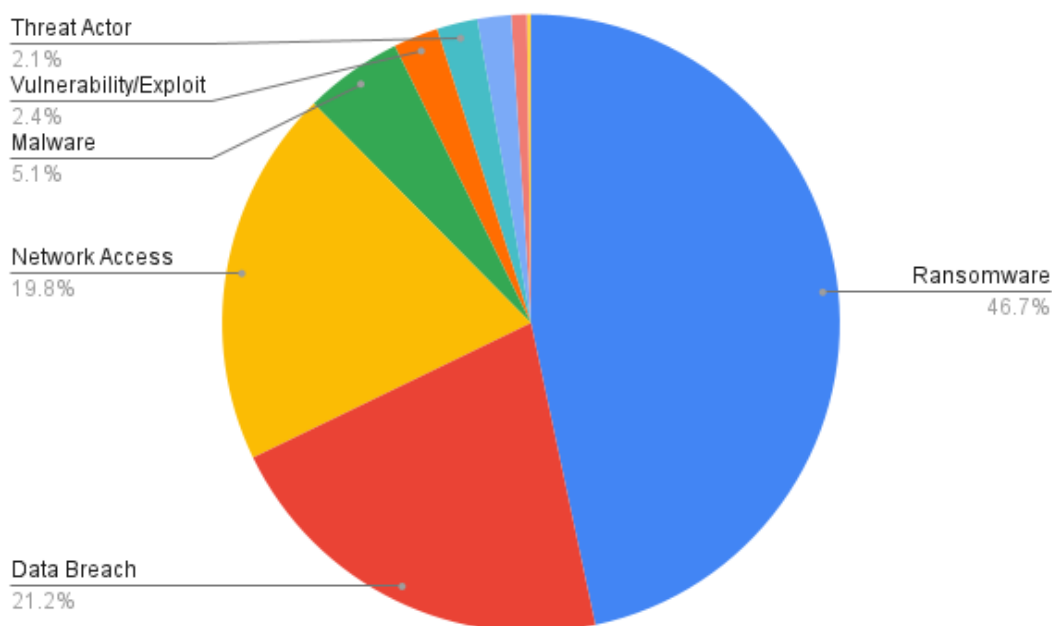


Figure 12. Distribution of activity on cybercriminal underground networks and forums

Source: ZeroFox Threat Research

The emergence of the RAMP

On July 13, 2021, ZeroFox observed that a Tor domain previously used to host the Babuk and later Payload.bin leak sites had become a new forum called RAMP. Forum administrator TetyaSluha, also known as Orange, stated that the forum was created in response to other forums announcing a ban on ransomware discussions. It did not take long for RAMP to attract well-known threat actors to the site, as the group behind LockBit (now LockBit 2.0) advertised their affiliate program on August 19, 2021, as seen in Figure 13. A representative for REvil also joined the forum on September 9, 2021, causing controversy after their disappearance in July.

While the Exploit and XSS forums have loosely held to their word of banning ransomware discussions, the administrator for Raid Forums later updated their announcement to claim that their post was made as a joke.

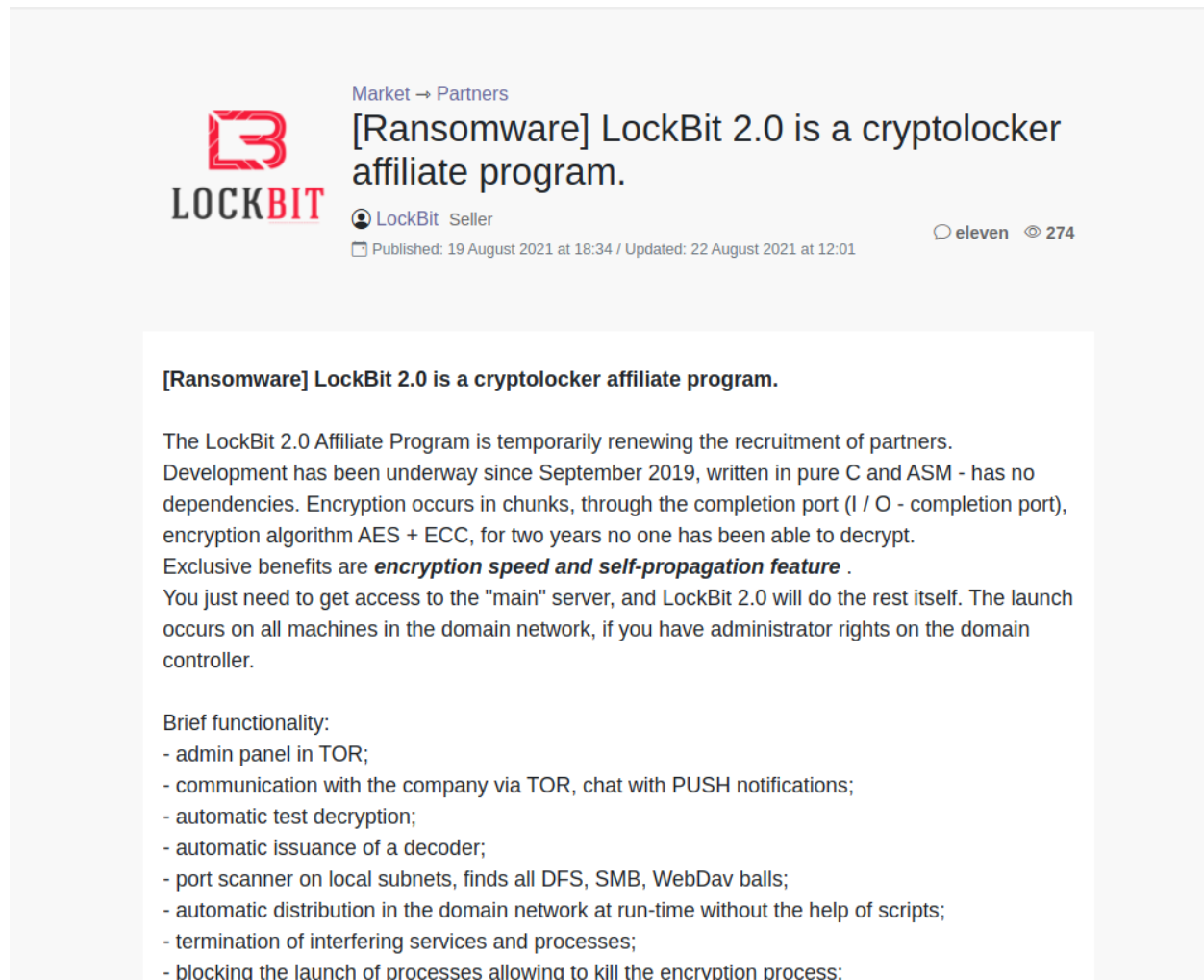


Figure 13. Actor LockBit advertising their affiliate program on the RAMP cybercrime forum.

Source: ZeroFox Threat Research

Personally Identifiable Information Leaks

ZeroFox also regularly monitors ransomware leak sites and underground forums for personally identifiable information (PII) being sold or leaked for free. Ransomware accounted for a vast majority of ZeroFox-observed leaks in Q3 by posting stolen data from victim organizations that refused to pay the demanded ransom. Ransomware is not the only source of data leaks, however. In addition to the usual credential leaks or database dumps exposing end-user account credentials and PII, threat actors are buying and selling access to various organizations' networks which can assist skilled and unskilled actors alike in infecting networks.

Compromised Credentials

This quarter saw over 72 million unique credentials from data breaches leaked online from 52 different organizations. IndiaMART, an India-based e-commerce company, had the largest number of unique records leaked at more than 20 million released in August 2021. Epik, an American domain registrar and web hosting company, had notable exposure when over 15 million unique credentials were dumped online.

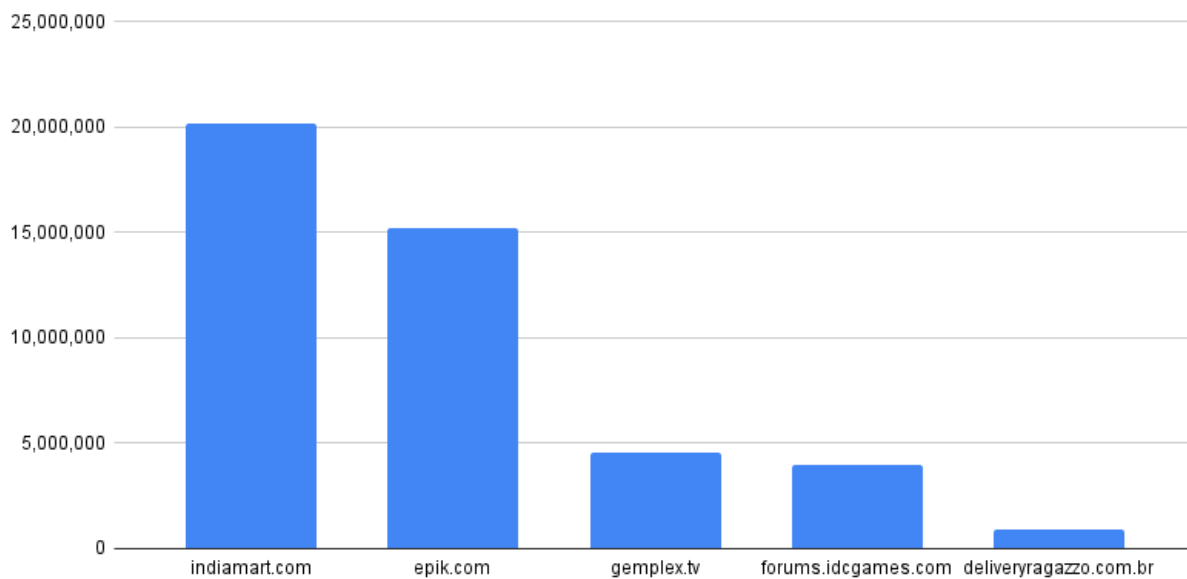


Figure 14. Five of the largest credential packages observed by ZeroFox in Q3 2021.

Source: ZeroFox Threat Research

Network Access Requests and Sales

Over the last quarter, ZeroFox observed a nearly 43% increase in activity around buying and selling network access. In cases where the target industry or organization was specified, manufacturing and technology tied for the top spot with roughly 17% of recorded activity each. The US and Canada once again took the top spot with over 26% of the requests observed by ZeroFox. In total, ZeroFox observed 269 network access requests and sales.

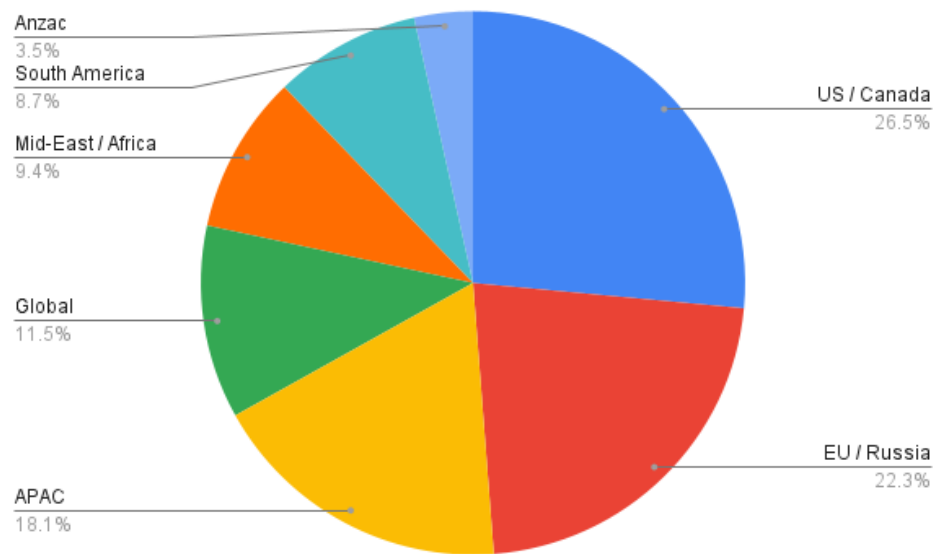


Figure 15. Network access requests and sales by target region in Q3 2021.

Source: ZeroFox Threat Research

Data Breaches

Epik

On September 14, 2021, the DDoSecrets leak site posted a data breach package targeting the organization Epik, an American domain registrar and web hosting company. In the post, the leaker claimed to have stolen a "decade's worth of data." Sales records included in the leak show what some scammers are willing to pay for typo-squatting domains. Some domains like "conibase.com," registered to mimic Coinbase, sold for more than USD 16,000. Between November 2020 and February 2021, one individual from Brazil paid over USD 200,000 to register typo-squatting domains. ZeroFox was able to extract 15,205,808 unique email addresses from this breach.

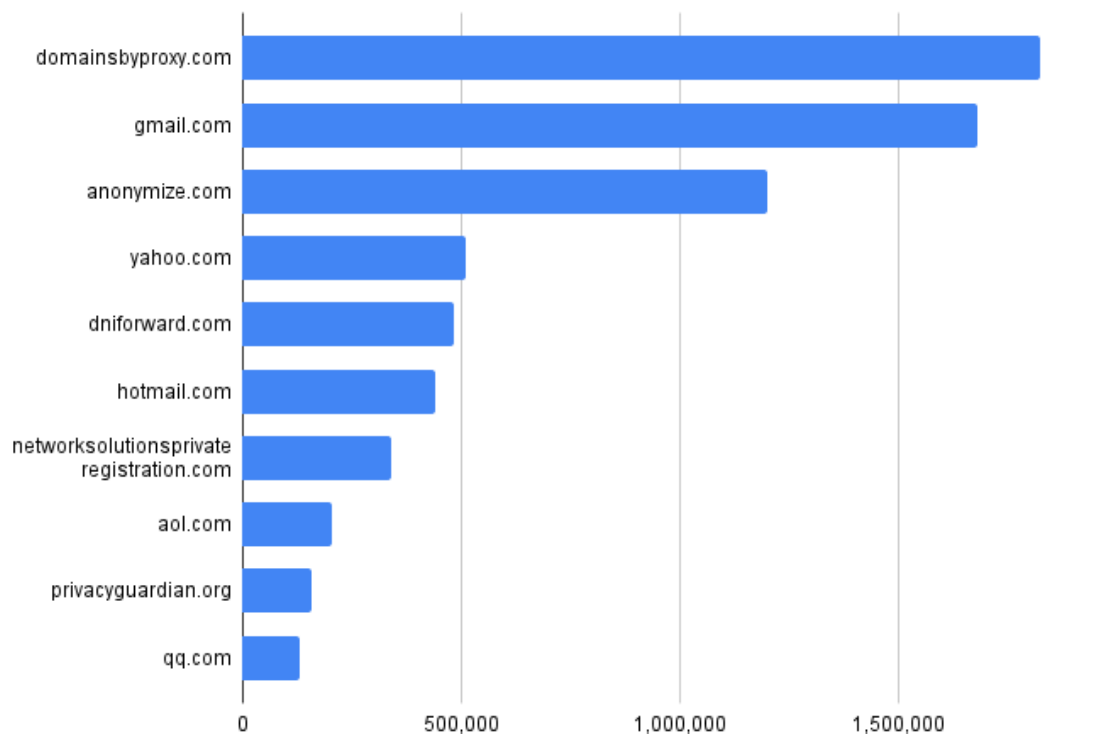


Figure 16. Top ten email domains discovered in the Epik data breach.

Source: ZeroFox Threat Research

Twitch

On October 6, 2021, ZeroFox observed the actor "Anonymous" on the English-language discussion board 4chan leaking the first part of allegedly compromised data from Twitch, a video live streaming service. The initial release contains source code from almost 6,000 internal Git repositories with commit history going back to its early beginnings. Source code for proprietary SDKs, services powering Twitch mobile, desktop, video game console clients, and many other Twitch-owned properties are included in the data released, including an unreleased competitor to the PC gaming platform Steam. In addition to code, records showing all payouts to streamers on the platform dating back to 2019 were included as well.

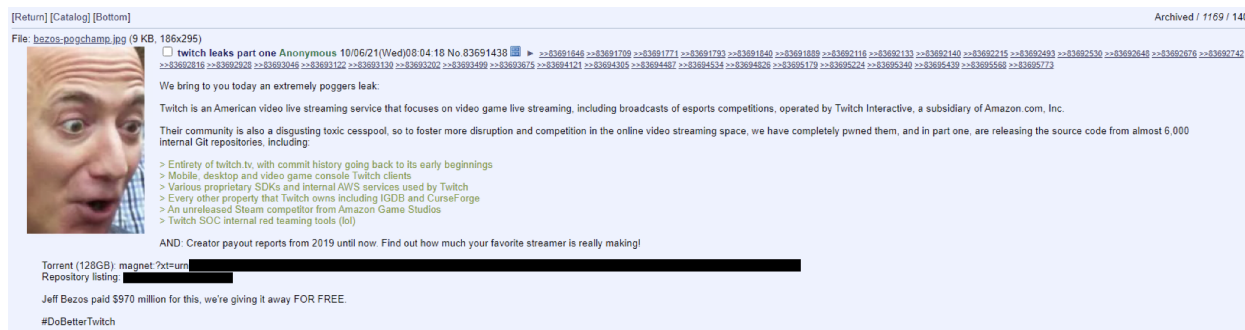


Figure 17. 4chan post with a torrent link and details about data found in the Twitch leak.

Source: ZeroFox Threat Research

Pandora Papers

The International Consortium of Investigative Journalists (ICIJ), a non-profit network of journalists, released a joint investigative report known as the Pandora Papers detailing the financial records of more than 330 politicians, public officials, world leaders and more across the globe. The data contained over almost 12 million financial records leaked from offshore service providers. The ICIJ shared their findings with 150 media partners on October 3, 2021. Reports that followed soon after have led to calls for investigation into those involved, and, in some cases, for their resignation. Those named in the reports have been accused of using shell corporations not only to hide money, but to finance mansions, property and other assets.

Recommendations

Due to persistent ransomware attacks, novel 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

Thus far in Q3 2021, threat actors once more proved how the global cyber threat landscape is evolving through novel threats and improved TTPs. As malware operators launched updated tools and technologies in attack chains, ransomware groups continued operations using both rebranded and revived ransomware variants. In response to these threats, governments around the world strategized plans and initiatives to form a robust response to cyber threats, including prevention methods by creating cyber security-focused agencies and organizations. ZeroFox Threat Research recorded over 10,000 unique mentions of vulnerability disclosures this quarter affecting enterprise organizations and their cohorts, which demonstrated the importance of patching and updating vulnerable systems, as well as the need to strategize additional ways to defend against such security vulnerabilities. Underground marketplace networks persisted in cybercriminal activity, and the addition of the RAMP forum presents a new community for threat actors to advertise and conduct criminal activity. Moreover, other cybercriminal forums advertised special phishing kit services that steal information from locked mobile devices indicating new types of fraud activity before the upcoming winter holidays. With only a few months remaining in 2021, it becomes clear that the threat landscape will continue to evolve making it critical for businesses and individuals to be vigilant for the remainder of 2021.