Threat Highlights Report

September 2022

WITH secure

Contents

Foreword

WithSecure's monthly threat highlights report contains our own proprietary data, as well as other carefully curated sources from the wider cybersecurity industry. It is designed to serve as a single-source product, providing an overview of this month's cybersecurity news, the changing threat landscape, and relevant advice.

This month's report contains a look at recent cyber-attacks on Albania, carried out by Iran-backed threat actors, as well as the hacks of Uber and Rockstar which have allegedly been carried out by LAPSUS$ hacker "Tea Pot" (aka, White/Breachbase), and we also examine the connection between Russian "hacktivist" groups and the GRU.

We assess the ransomware threat landscape, which includes a look at LockBit, who have recently paid out as part of their bug bounty and had code for their builder leaked, as well as examining relative newcomers Sparta and BianLian and discuss the growing trend of ransomware groups targeting government networks. Additionally, if you have ever wondered what it is like to negotiate with a ransomware group, we recommend having a go at this interactive game available on the Financial Times website.

We also take a brief look at a number of issues, including the Raspberry Robin worm being spread through the usage of USB drives in print shops, a new botnet called MooBot which is being installed on compromised D-Link devices, a threat actor who is specifically targeting US schools, and a valuable report on the state of internet-connected things by Censys.

- Ziggy Davies

1 Monthly highlights

1.1 Iran attacks Albania

Tensions between Iran and Albania have increased since about 2013 when Albania started allowing members of the People's Mujahedin of Iran (MEK) to take refuge in the country, an organization Iran views as a terrorist group. This culminated on July 15th 2022 when Albania experienced a severe cyberattack that resulted in the shutdown of several government services and websites, which was followed by a further attack in September that caused the temporary closure of border control services.

Researchers from Mandiant were the first to attribute the July attack on Albania to Iran, assessing "with moderate confidence that one or multiple threat actors who have operated in support of Iranian goals are involved". Mandiant was able to analyze 3 pieces of malware related to the attack, including:

- ROADSWEEP, a ransomware variant used to encrypt systems
- CHIMNEYSWEEP, a backdoor that supports taking screen-shots, listing/collecting files, spawning reverse shells, and keylogging, as well as utilizing telegram for its C2.
- ZEROCLEAR, a destructive wiper.

The ROADSWEEP ransomware dropped a politically themed ransom note on systems and the attack was also claimed by a front organization called "Homeland Justice", a ruse designed to suggest that the attack was carried out by Albanian citizens in opposition to the government.

Albania investigated the July attack in cooperation with Microsoft's Detection and Response Team (DART), with Microsoft releasing their findings publicly, which further attribute the attack to threat actors sponsored by the Iranian government. With regards to attribution, Microsoft's forensic analysis indicates:

- *"The attackers were observed operating out of Iran.*
- *The attackers responsible for the intrusion and exfiltration of data used tools previously used by other known Iranian attackers.*
- *The attackers responsible for the intrusion and exfiltration of data targeted other sectors and countries that are consistent with Iranian interests.*
- *The wiper code was previously used by a known Iranian actor.*
- *The ransomware was signed by the same digital certificate used to sign other tools used by Iranian actors".*

The point of initial access for attackers was the exploitation of a vulnerability (CVE-2019-0604) in an unpatched SharePoint server, which occurred in May 2021, with escalation or privileges occurring in July 2021. Between initial access and May 2022, threat actors were observed to exfiltrate mail data using the tool Jason.exe, a tool associated with the Iranian Ministry of Intelligence. This activity was followed up with the detonation of ransomware and a wiper, which fits the previous tactics, techniques, and procedures (TTPs) used by Iran, and can be further attributed as the wiper contains a license key previously used in a 2019 attack, which was orchestrated by Iranian-sponsored threat actors.

While little information is known about the later attack which resulted in the shutdown of Albania's border crossing information systems, Albania has said it came from the same source, blaming Iran. We can assume that the incident involved the same ransomware/wiper TTPs, due to the destructive nature of the attack and the period of recovery that followed.

In response to the attack, Albania's Prime Minister Edi Rama published a video statement on YouTube, informing citizens of Albania and the wider world, that they were blaming Iran for the attack and severing diplomatic relations with the nation, informing Iranian diplomats in the nation that they had 24 hours to close their embassy and depart Albania. The United States has supported Albania throughout its investigation

and has also made statements condemning Iran's actions, and promising "*further action*". Days later the US unsealed an indictment issued by the Department of Justice, which charges three Iranian nationals with carrying out ransomware attacks on organizations linked to US critical national infrastructure, among others, and also placed sanctions on 10 individuals and two entities associated with Iran's Revolutionary Guard Corps (IRGC) and ransomware attacks.

WithSecure™ Insight

The activity carried out by Iranian-sponsored threat actors is highly unusual, and nation-state ransomware/wiper activity like this has previously been limited to cyber warfare perpetrated by Russian-backed threat actors on entities within Ukraine and use of ZEROCLEAR(E) by Iran-backed actors on the middle-eastern energy sector. Iran's actions in attacking a nation during peacetime is significant.

The attack in July 2022 had a dramatic effect on mobilizing fellow NATO nations in addressing Iran as a hostile threat actor and has led to statements from the US and UK condemning the actions of the nation. It also provided the wider security community the opportunity to analyze Iran's TTPs and toolkit, with Certfa, ClearSky, Microsoft, and CISA all releasing reports and advisories on Iran-adjacent threat actors in recent weeks. This helps defenders immensely, as it provides insight into these groups' attack pathways and TTPs, enabling defenders to build better defenses and increase preparedness.

The attack by Iran on Albania is almost certainly politically motivated and is in direct response to Albania's decision to give refuge to members of MEK, highlighting how world events can drive an asynchronous response in cyberspace. While Iran is known to be hostile to Albania, Israel, and the US, any shift in geopolitics involving Iran or their interests could certainly result in more nations finding themselves within the scope of hostile Iranian cyber activity.

But in addition to this, we have also gained insight into the link between Iran and financially motivated activity associated with ransomware, showing an overlap in the motivations and capabilities of the nation and the threat actors they sponsor.

What can you do?

While this event is troubling and signals an escalation in Iran's hostile cyber activity, it has provided us an opportunity to learn about relevant TTPs and increase preparedness.

This includes:

- Ensuring that vulnerabilities are patched, especially those with known exploits, such as CVE-2018-13379, CVE-2020-12812, CVE-2019-5591, CVE-2021-34523, CVE-2021-31207, CVE-2021-34473, CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105.
- Raising awareness surrounding the use of social engineering and the abuse of platforms like LinkedIn by threat actors seeking to gain initial access and/or conducting espionage.
- Creating and maintaining incident response plans that consider encryption/destruction of data/systems and how these would be restored.
- Consider the information security CIA triad (confidentiality, availability, integrity), when storing data, and assess what the result and risk will be if data is compromised.

There is a lot of tension surrounding Iran and geopolitics, including internal turmoil, and any relationship that involves Iran or one that is adjacent to its interests could bring an organization within the scope of hostile cyber activity, as such these relationships should be examined and resultant risks be considered.

1.2 Uber and Rockstar breached by “Tea Pot”

On September 15th 2022 transportation service provider Uber was hacked, and speculation surrounding the identity of the hacker, suggests it was carried out by a 17-year-old member of the LAPSUS$ gang going by the moniker “Tea Pot” (aka White, BreachBase), whose motivation is unknown.

The first indication of an issue at Uber, was a widely shared screenshot of the hacker posting a message to Uber’s internal Slack, stating:

“I announce I am a hacker and Uber has suffered a data breach…”

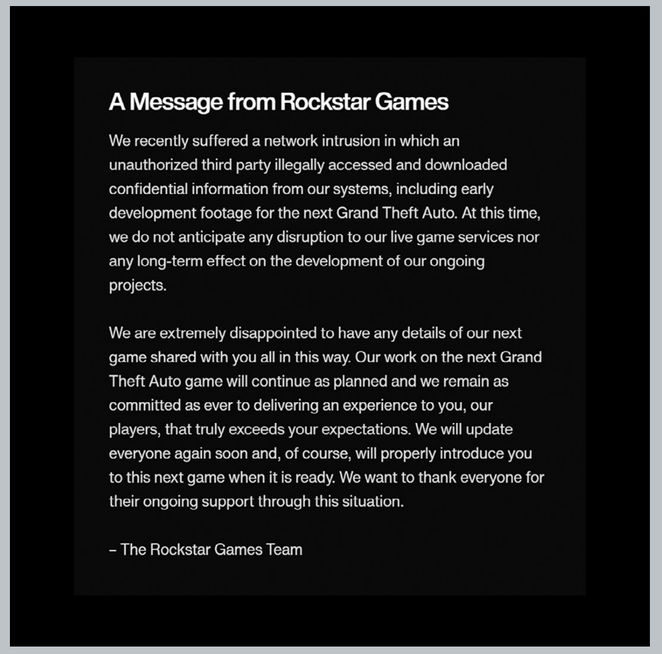
The message appears to have been interpreted as a joke/hoax initially, but Uber have since announced the hack as genuine. Uber has continued to provide updates on the situation using their online newsroom and on September 19th provided a thorough update, explaining:

- *“The attacker gained access by using compromised credentials which were likely sold on the dark web, and had been compromised due to malware.*
- *The account was protected by MFA, but the attacker used an MFA fatigue technique, which resulted in the employee accepting a push notification and inadvertently providing access to the attacker.*
- *The attacker was then able to access other Uber employee accounts and gained privileged access to several internal tools, G-Suite and Slack.*
- *Uber believes the attacker(s) is a member/affiliate of the LAPSUS$ hacking group.*
- *Uber is currently analyzing and assessing the impact of the hack, and looking at what data was exfiltrated, but do not believe any sensitive customer data was accessed”.*

The hacker has openly bragged about the incident on messaging service Telegram, and has even shared part of their attack methodology, stating that they escalated privileges by accessing stored Powershell scripts that “contained the username and password for an admin user in Thycotic..”.

Days later, material belonging to video game publisher Rockstar Games began to leak across social media and on forums, with the data containing videos of the upcoming game Grand Theft Auto 6. The origin of this leak was a GTA forums user with the username “teapotuberhacker”, clearly linking the incident at Uber with the later hack of Rockstar.

Rockstar later posted a statement on Twitter regarding the incident, confirming the data as genuine and expressing disappointment:



While Rockstar has not attributed the incident, or provided details surrounding initial access, the circumstances, timing, and claims from “Tea Pot”, clearly link the breach at Uber and Rockstar.

There is speculation that a recent arrest by the UK City of London Police is connected to the incidents, but no official statement has been made.

WithSecure™ Insight

While many hacks involve the exploitation of vulnerabilities and demand technical knowledge and prowess, many others do not, and the hacks or Uber and Rockstar highlight this. In the incident against Uber, it would appear that initial access was gained through the purchase of legitimate credentials that had previously been compromised, likely using stealer malware such as Vidar or Racoon. While MFA was enforced on this account, the hacker was able to bypass this using a social engineering technique which we have previously reported on called "*MFA fatigue*", which involves the spamming of push notification requests to the associated mobile device. WithSecure™ have detected this technique ourselves, and have investigated incidents which attempt to gain access in this way, highlighting it as an ongoing issue that has been widely adopted by threat actors. If claims are true about the method of initial access, it is another reminder that often the vulnerability that gets exploited is the human and while it is easy with hindsight to suggest that a product or service may mitigate against such attacks, technology alone, or specific configurations therein cannot be considered a silver bullet solution.

While information regarding the initial access of Rockstar is not as widely available, the association with "*Tea Pot*" and LAPSUS$ suggests that access was likely gained in a similar way, and LAPSUS$ are known to favor the purchase of compromised credentials and social engineering when gaining initial access, rather than engaging in the development and exploitation of vulnerabilities/0-days.

A list of known LAPSUS$ victims includes:

- Brazil's Ministry of Health
- Okta
- Nvidia
- Samsung
- Mercado Libre
- Ubisoft
- T-Mobile
- Microsoft, and
- Globant

The arrest of a 17-year old from Oxfordforshire by the City of London Police, while not confirmed as linked to the breaches of Uber and Rockstar, certainly coincides with the breaches, and the data released about the individual fits with the profile of LAPSUS$ member "*White*" (aka, BreachBase) who is allegedly the same person as "*Tea Pot*".

What can you do?

Both of these incidents highlight the importance of proper MFA enforcement and the risk posed by MFA fatigue attacks and social engineering. The method used for MFA enforcement is vital, and the use of push notifications in mobile authentication apps is a known issue. WithSecure™ highly recommends the use of other MFA approval methods, such as number matching/challenge questions, or the use of hardware MFA solutions. SMS or phone call options are not recommended, due to the risk of SIM-swap attacks, which have also been abused by LAPSUS$ in the past (among others).

The training of personnel is also paramount, and the risk of credential theft, MFA attacks and social engineering should be explained, and adequate cybersecurity and operational security training be provided. This also includes ensuring that all personnel know what to do in the event of a breach and who to contact, as in the case of Uber, it appears many employees mistakenly mistook the Slack breach for a joke/hoax.

The incident at Uber has also highlighted an issue, as admin user credentials had been included in a Powershell script, which was accessible by a lower privilege account. WithSecure™ note that the inadvertent leaking of credentials in this way is quite common, with code often containing sensitive information and credentials that could, in the wrong hands, be abused. Access to this sort of data should always be restricted, and code with embedded credentials should be avoided if possible and alternative solutions explored.

1.3 Russian ‘hacktivist’ groups have close ties to GRU

Google subsidiary and cybersecurity firm Mandiant have shared research surrounding the link between several self-proclaimed Russian hacktivist groups and the Russian intelligence services (GRU). Mandiant believe that the groups “*Xaknet*”, “*Infoccentr*” and “*CyberArmyofRussia_Reborn*” are all coordinating their operations with the GRU, and have based this finding on the use of tools/malware linked with APT28 and Sandworm, who are GRU sponsored/adjacent threat actors, and the subsequent leak of data connected to those breaches by hacktivist groups.

The three groups monitored and researched by Mandiant, all operate publicly accessible Telegram channels, on which they promote disinformation/narratives in support of Russia and the invasion of Ukraine, and share data which has been compromised during hacking activity linked to APT28 and Sandworm, and therefore the GRU. This connection leads Mandiant to believe that the operators/moderators behind the Telegram groups are either Russian intelligence officers, or at least cooperating with the Russian intelligence services.

Throughout the invasion of Ukraine and ongoing war, there have been a myriad of groups carrying out cyber activity and attacks on both sides of the conflict. An independent security researcher has been tracking these groups and regularly updates the threat landscape via Twitter, and there are currently 84 active groups (35 pro-Ukraine, 43 pro-Russia, 5 unknown) tracked.

WithSecure™ Insight

Hacktivist groups ordinarily perform low-level and disruptive cyber-attacks, such as DDoS, defacements and the distribution of disinformation/propaganda, with many operating Telegram channels or social media sites to coordinate their operations and disseminate materials.

The attacks involving CADDYWIPER were highly sophisticated and were well outside the capability of many of hacktivist groups, and at the time were directly attributed to both APT28 and Sandworm, threat actors linked to the GRU. Mandiant’s findings that hacktivist groups have been leaking data gained during the CADDYWIPER attacks, is indicative of a relationship between Russia and certain hacktivist groups, though the full extent of this relationship is unknown.

WithSecure™ have reported on pro-Russian hacktivist groups several times throughout the year, and have always questioned their provenance and connection to the Russian intelligence services, especially with many groups showing an increase in capability including the use of botnets.

What can you do?

Hacktivist groups target organizations and nations based upon the current geopolitical landscape and their agenda, with pro-Russian groups like Xaknet, Killnet, Killmilk, etc all engaging entities that are either associated with Ukraine, or are relevant to the interests of Russia.

Recent disruptive activity in Norway, Lithuania, Germany, Italy and Romania has all been attributed to pro-Russian hacktivist groups, and they can pose a significant threat and risk to organizations within nations that are aligned with Ukraine, the United States and/or NATO.

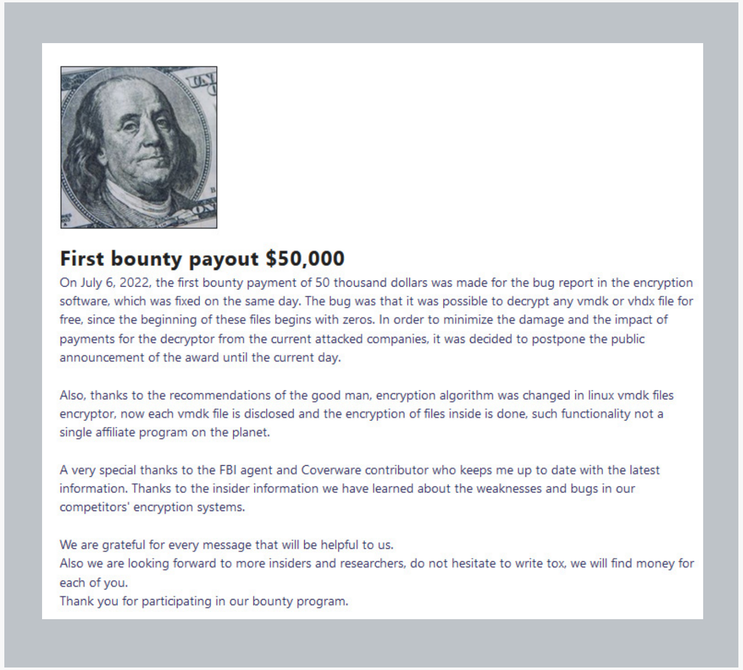
With regards to the activity that links these groups to APT28 and Sandworm, defenders should familiarize themselves with the TTPs commonly used by the groups, and take relevant mitigations including:

- Patching software, services and assets, as to prevent the exploitation of vulnerabilities.
- The enforcement of MFA (number matching/challenge questions or hardware solutions).
- Reduce exposure of internet facing services such as VPN and RDP and closely monitor them.
- Provide training to personnel on social engineering, phishing, malicious documents and how to properly report incidents.

2 Ransomware: Trends and notable reports

2.1 LockBit bug bounty and leaks

Ransomware group LockBit, who recently announced their own bug bounty program, welcoming the examination and testing of their tooling, have announced their first bug bounty payment.



The group report that they paid $50,000 to an unnamed person who identified an issue in their encryption process, which enabled the trivial decryption of .vmdk and .vhdx files.

This program and activity is highly unusual, and LockBit are trying to 'legitimize' their operation by emulating the security practices of legitimate (and more progressive in cybersecurity) businesses by carrying out a bug bounty program. It's important to remember that LockBit are cybercriminals and that nothing they do is legitimate or lawful, with LockBit attacking several organizations every day, causing damage, disruption and financial impact which can be hard to recover from.

On September 21st 2022 LockBit experienced a leak of their own when the builder for their 'LockBit Black' variant was leaked, and then made available via GitHub. The builder has been analyzed by a researcher at Cyber Geeks, who provide a technical deep-dive on the processes and capabilities of the builder.

This leak will undoubtedly cause problems for LockBit, but it so far has not slowed their operations, with attacks still occurring on a daily basis. What is likely, is the adaptation of the builder to create independent forks of the LockBit builder, which will be utilized by other threat actors, much like how the leak of Conti's source code led to its use by other ransomware groups, with ransomware group "*Bl00dy*" already adopting the leaked code.

2.2 Sparta ransomware

On the 13th of September 2022, a new ransomware leak site on the dark web was detected, with the site belonging to a new ransomware threat actor going by the name "SPARTA".

Currently, the site is very basic but hosts data relating to 22 potential victims. With 19 (86%) being geographically located within Spain, indicating a specific focus of the ransomware groups targeting and victimology. The victims come from various sectors, suggesting the group is less concerned with industry when deciding on targets.

As this group is very new, little information or intelligence regarding their attack methodology, tactics, techniques, or procedures is known. WithSecure™ will continue to monitor this threat actor and may provide updates, as more information becomes available.

Many ransomware threat actors gain initial access through malicious spam (malspam), theft of legitimate credentials, breach of exposed RDP/VPN services, or exploitation of vulnerable services. As such, we highly suggest that phishing and social engineering awareness is a priority, and the patching of services/products be carried out with a risk-averse patch management plan.

Organizations should have incident response plans and playbooks, which are focused on the theft and encryption of data. This includes data held by third parties, and in this case, especially those who are geographically linked to Spain.

2.3 Nations targeted by ransomware

In recent months there has been a growing trend of government networks and national infrastructure being targeted by ransomware actors, especially in South America and the Balkan's. Attacks have occurred on:

- Parliament of Montenegro
- Parliament of Bosnia and Herzegovina
- The Dominican Agrarian Institute of the Dominican Republic
- Government of Chile
- Judiciary of Chile
- The legislature of Buenos Aires, Argentina
- Financial department of Rio de Janeiro, Brazil

These attacks have been perpetrated by different threat actors, in what appears to be a growing trend of financially motivated targeting of nation states.

2.4 BianLian ransomware

Researchers from Cyble and [redacted] (that's actually the company name) have recently released analysis on a ransomware group/variant called BianLian first observed in July 2022.

The group appear to be focused on gaining initial access through the exploitation of ProxyShell vulnerabilities, but their victimology is not limited to a specific sector with attacks occurring on 24 organizations between 14th July 2022 and 13th September 2022.

2.5 Ragnar Locker deep dive

Ransomware group Ragnar Locker, who have been active since at least June 2020 have recently attacked a gas pipeline company in Greece, in scenes reminiscent of the attack Colonial in the United States.

The SOC team at Cybereason have released an analysis of Ragnar Locker following the Greek attack, which also discusses other attacks on the energy sector and related critical national infrastructure, a sector that is seen as a legitimate target by ransomware actors.

2.6 Technical analysis of Redeemer

Threat researcher Mehardeep Singh Sawhney of CloudSEK has released a technical analysis of ransomware variant Redeemer.

The ransomware, which has been active since September 2021 has recently been updated to version 2.0 and is being promoted on the dark web and hacker forums. The ransomware includes GUI elements which appear to make its usage by affiliates simple and may therefore appeal to a non-technical audience. In all other areas, Redeemer is a typical ransomware variant which is capable of quickly encrypting entire systems, and inhibiting recovery.

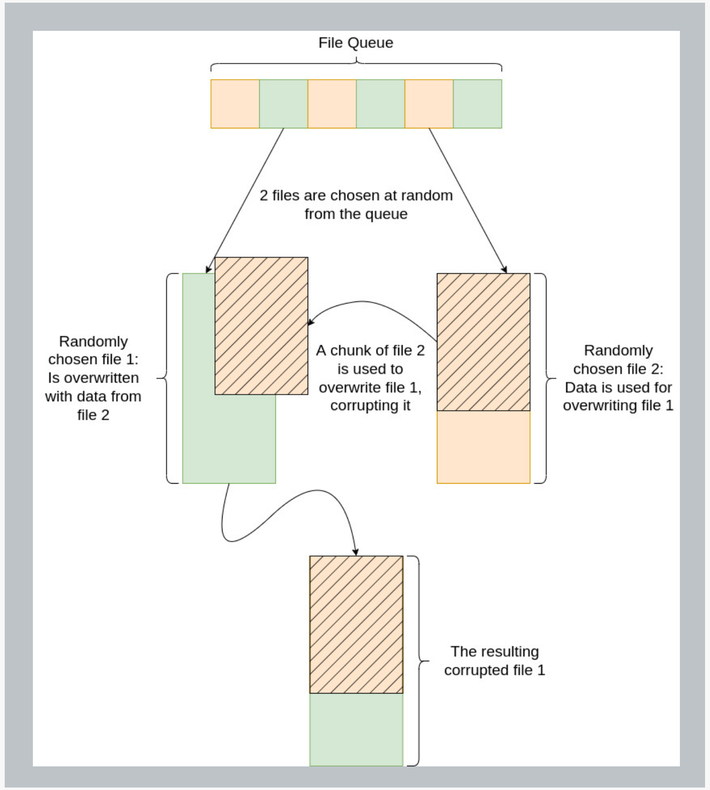
2.7 ExMatter for exfiltration and corruption

ExMatter, an exfiltration tool which has been used by ransomware operators since at least September 2021 now includes a feature which when enabled, corrupts data once it has been exfiltrated, mitigating the need for a separate encryption phase in ransomware attacks.

ExMatter has recently been discussed and analyzed and its basic function "*sync*" is made to identify and exfiltrate common file types based upon their extension, which include:

- PDF
- DOC
- DOCX
- XLS
- XLSX
- PNG
- JPG
- JPEG
- TXT
- SQL
- BMP
- RDP
- MSG
- PST
- ZIP
- RTF
- IPT
- DWG

The new function, which is dubbed "*eraser*" runs concurrently with sync and essentially partially overwrites files with data from other files on the system, corrupting them.



Ransomware operator BlackCat (ALPHV) are currently using this new version of ExMatter and it is believed to still be in development. The motivation for this shift towards a tool that corrupts data after exfiltration, rather than encryption, is likely a desire to streamline the attack process, saving time and effort, as well as aggravating file recovery through the development of decryptors.

3 Other notable highlights in brief

3.1 Raspberry Robin spread through print shops

Little is known about Raspberry Robin, a worm that was first identified by Red Canary in September 2021. But it is thought to be developed by the cybercrime group Evil Corp, and primarily infects QNAP devices.

The initial access for incidents involving Raspberry Robin is known to be infected USB drives, which contain a malicious LNK file, which spawns malicious commands on interaction. But recent research suggests that these USB devices are being infection via usage at print shops and other public locations. How these print shops have become a hive of Raspberry Robin is unclear, but it highlights the need for good USB security and sanitation, this includes:

- Not using work USB devices with devices outside of your enterprise environment (including personal computers).
- Using printers within your own enterprise environment, directly rather than via external device.
- If you must use a USB stick for printing, use one in a "read-only" mode either through hardware switch or utility such as DISKPART.
- Ensure that USB sticks are scanned by appropriate security solutions.

3.2 Censys state of the internet

Censys, a web-based search platform for identifying potentially vulnerable connected devices has released an annual report titled "*2022 State of the Internet*". The report contains a look at:

- What are the major services running on the web and where are they hosted?
- An overview of risk and vulnerability and the response to new issues.
- A look at 37 organizations attack surfaces to understand internet footprints.

Findings by Censys include:

- *"Misconfigurations–including unencrypted services, weak or missing security controls (Content Security Policy (CSP), etc.), and self-signed certificates–make up roughly 60% of the risks we observe across the Internet. Exposures of services, devices, and information represent 28% of observed risks in our data, and Software Vulnerabilities represent 12% of risks observed in 2022.*
- *With so many organizations migrating services to the cloud, there's a lot of attention on cloud security and exposure. However, there's still significant exposure risk for on-premises infrastructure. The majority of the Internet hosts and services do not run on a major cloud provider, but rather are hosted on-premises or in a conventional datacenter. Despite increasing cloud adoption, internet exposure isn't just a cloud problem.*
- *Vulnerability management continues to pose challenges. Research suggests that generally, it takes over 200 days to patch severe vulnerabilities, and we observed three distinct types of behavior in response to vulnerability disclosures: near-immediate upgrading (Log4j), upgrading only after the vulnerability is being actively and widely exploited (GitLab), and near-immediate response in the form of taking the vulnerable instance off the internet entirely, or in other cases, patching (Confluence).*
- *Organizations have an average of 44 different domain registrars and presence in 17 different hosting providers (including cloud, datacenter, and on-premises equipment). A reported 59% increase in shadow IT, driven by remote work demands over the last 2 years, has likely contributed to this sprawl. Organizations must continue enabling their employees, but this can lead to visibility issues when IT and Security teams are left out of the conversation".*

3.3 MooBot leverages D-Link vulnerabilities

Researchers at Unit 42 have released analysis on a Mirai botnet variant called "*MooBot*", that is being used to target vulnerable D-Link network devices.

Attackers are exploiting four known vulnerabilities within D-Link devices, which include:

- *"CVE-2015-2051: D-Link HNAP SOAPAction Header Command Execution Vulnerability*
- *CVE-2018-6530: D-Link SOAP Interface Remote Code Execution Vulnerability*
- *CVE-2022-26258: D-Link Remote Command Execution Vulnerability*
- *CVE-2022-28958: D-Link Remote Command Execution Vulnerability".*

Upon compromise, the attacker(s) are able to fully control the devices as part of a botnet, and can use that infrastructure to carry out other attacks such as DDoS. Exploitation of all of these vulnerabilities is trivial, so patches and mitigations should be deployed with urgency.

3.4 BEC group targets schools

As a new school season has begun, threat actors are targeting the education sector, with a campaign by a threat actor called "*Chiffon Herring*" being detected by the team at Abnormal Security.

The group reportedly target educational establishments within the United States, and begin their attack by impersonation of a genuine school employee such as a teacher. This is done through email spoofing, which is possible due to the lack of DMARC enforcement and begins with an email to the schools finance department/officer, asking to change the employees bank details for payroll. This sort of attack is known as "payroll diversion" and is a basic form of Business Email Compromise (BEC) and if successful, leads to the diversion of employees salaries to attacker controlled accounts.

The best way to combat this type of attack is:

- Enforcement of DMARC and other domain protection standards.
- A strict procedure on changing banking details for employees, that is not simply an email.
- Email filtering and use of security products such as AV.
- Providing staff with training on social engineering, BEC and common phishing techniques.

4 Threat data highlights

4.1 Exploits

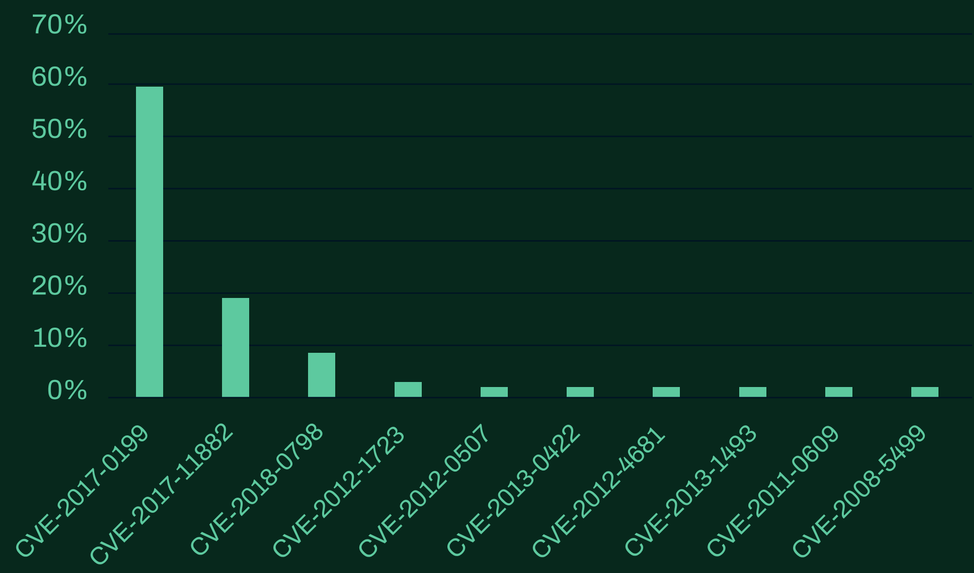
WithSecure™ telemetry shows that threat actors continue to favor older but proven exploits, with exploits for CVE-2017-0199 and CVE-2017-11882 continuing to top the board.

CVE-2017-0199 was the most prevalent vulnerability exploited at endpoints during September. It is a remote code execution vulnerability in MS Office and Wordpad exploited by a specially crafted RTF document.

CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker, it is exploited by malicious office documents.

In September, CISA added 22 new vulnerabilities to their known exploited list. These include vulnerabilities in various applications, products and devices such as Apple operating systems, Microsoft Windows, Google Chrome and various providers of networking equipment.

Exploits in the wild

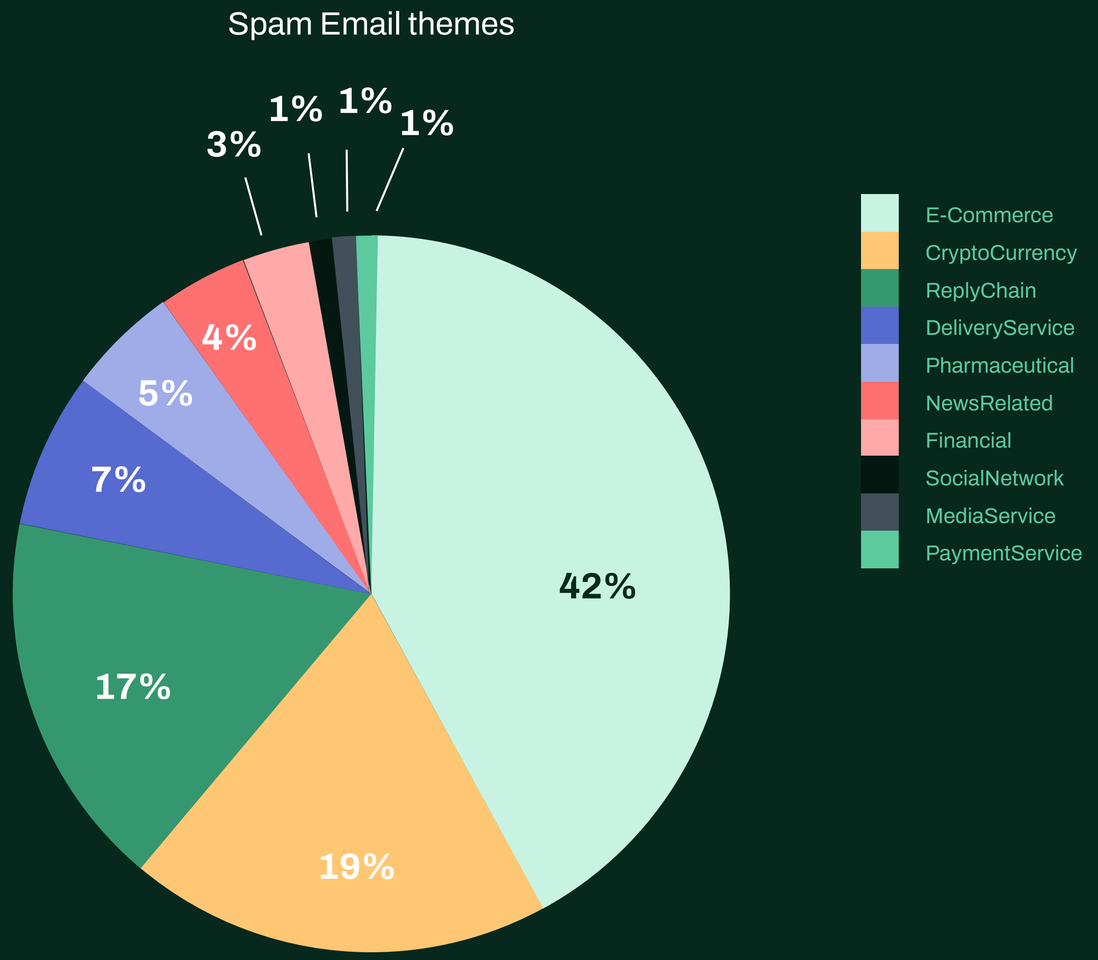


WithSecure™ endpoint protection

4.2 Email threats

In September, cryptocurrency themed emails have seen a slight increase from last month (12% to 19%), but of note is the considerable increase in “reply chain” style spam mail (4% to 17%) and considerable drop-off of financial themed mail (23% to 3%).

Reply chain spam mail involves attackers inserting themselves into legitimate conversation chains using compromised credentials, and can also be achieved by creating the illusion of a legitimate reply chain, by the fabrication of long email threads.



WithSecure™ spam data collection

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure