Threat Highlights Report

March 2022

WITH secure

Contents

1 Monthly highlights

1.1 Okta LAPSUS$ Compromise

On the 22nd of March the LAPSUS$ threat actor posted to their telegram channel claiming to have compromised the identity provider Okta. LAPSUS$ provided screenshots showing access to what appear to be internal systems of Okta. The screenshots all appear to show the date of the 21st of January 2022. WithSecure cannot independently verify these screenshots, but the CEO of Okta posted tweets appearing to confirm that a support engineer at a sub-processor had been compromised around that time. Okta later released a statement indicating that they did not believe there was any impact to Okta's customers as a result of the intrusion. This was then corrected by another statement that provided detail indicating that Okta believe 2.5% of its customers had been potentially impacted by the intrusion.

The LAPSUS$ threat actor has claimed that they have not dumped any databases from Okta and have stated that their focus was on Okta's customers, which contains a number of high-profile organizations globally. There is a screenshot included in their dump that appears to show the actor with access to an account that would allow them to reset its password, generate a temporary password, reset Multi-Factor Access (MFA), and alter groups of the account.

The LAPSUS$ threat actor appears to operate a financially motivated data extortion model, where they will steal data from organizations and demand payment not to release this data publicly. They have reportedly been involved in a number of high-profile breaches that has included Microsoft, NVIDIA, Samsung, and Ubisoft.

Microsoft have released a report in to the actor, who they track as DEV-0537, which provides insight in to the tradecraft the actor employs against its victims. The report details how the actor focuses on compromising user identities for initial access using the Redline password stealer, purchasing credentials from underground forums or employees at targeted organizations and searching public code repositories for credentials. With these credentials the actors then would attempt to access internet facing systems and bypass MFA where possible. The Microsoft provides further technical insights and notes the actors use of NordVPN in their data egress actions.

WithSecure™ Insight

Okta is commonly used by organizations to manage access to their cloud and SaaS applications. The intrusion poses a risk to those organizations notified by Okta as well as organizations they supply services for. As the threat actor has posted screenshots of this access and has shown the ability to gain access to other high-profile organizations, whether related or not to this compromise, it is a credible risk that WithSecure recommends organizations should take proportionate steps to mitigate. WithSecure assess that it is likely that the main risks from the LAPSUS$ threat actor is the theft of data for extortion or onwards access into customer environments.

Organizations concerned that they may have been compromised or wanting to build detection based on the tradecraft reportedly used by the LAPSUS$ threat actor should review the logging information provided by Okta and look to build use cases based on the Microsoft report as well as looking at open-source detection logic shared by Elastic and Sigma.

UK police confirmed they had arrested seven people in connection with a hacking group believed to be LAPSUS$. WithSecure is aware of wider open-source information on individuals but believes it is inappropriate to comment further due to the status of the persons involved.

1.2 Heightened Awareness of Russian Threat Activity

The United States (US) has once again called upon the private sector to be on guard and address vulnerabilities which are being targeted by Russian-backed threat actors. The statement by President Biden, comes as tensions increase between the US and Russia over the invasion of Ukraine and related sanctions, with specific mention of intelligence relating to Russia exploring the use of cyberattacks. President Biden states his "…administration will continue to use every tool to deter, disrupt, and if necessary, respond to cyberattacks against critical infrastructure. But the Federal Government can't defend against this threat alone. Most of America's critical infrastructure is owned and operated by the private sector and critical infrastructure owners and operators must accelerate efforts to lock their digital doors". Clearly outlining the danger that private companies who control Critical National Infrastructure (CNI) are potentially facing. The US Department of Justice (DoJ) has also taken the step of unsealing indictments which implicates four Russian nationals in cyber attacks against CNI, further thrusting Russia's cyber activity into public light.

The release of this statement was followed by a statement by the UK government, stating that the UK NCSC is almost certain that the Russian FSB is directly responsible for cyber attacks and malicious activity which is targeting UK CNI and its allies. The statement coincided with an alert by the US Cyber and Infrastructure Security Agency (CISA), which warns of Russian-backed threat actors exploiting the "PrintNightmare" (CVE-2021-34527) vulnerability.

CISA also warn about the configuration of Cisco's DUO multi-factor authentication (MFA) application, which is being actively exploited by the same threat actor to gain initial access. This is possible as DUO un-enrolls inactive accounts, but these can be easily enrolled with a new attacker-controlled device if the account is compromised. The alert contains a technical breakdown of the activities seen, as well as Indicators of Compromise (IOCs) and mitigation advice, including the adjustment of MFA configuration, the patching of known vulnerabilities and strong password policy enforcement.

CISA released a further alert relating to the current geopolitical landscape and tensions with Russia, which highlights the threat to satellite communication (SATCOM) networks posed by hostile state-backed threat actors. The alert follows disruption to Viasat Inc.'s KA-SAT satellite prior to the invasion of Ukraine, which is currently being assessed and may have been caused by an attack orchestrated by Russian-backed threat actors and designed to disrupt the military communications of Ukraine during the invasion.

Ukraine continues to be targeted by destructive malware with ESET analysts identifying a new wiper they have dubbed "CaddyWiper". The new wiper is the third instance of destructive malware targeting Ukraine in as many weeks, and appears to be part of an ongoing campaign targeting the nation and coincides with the ongoing invasion by Russia. While CaddyWiper shares no major code with the previous wiper malware samples HermeticWiper and IsaacWiper, the functionality is the same, being designed to destroy data and partition information on targeted system.

The Computer Emergency Response Team of Ukraine (CERT-UA) have detected a further instance of destructive malware they have named "DoubleZero". Which is an obfuscated .NET program designed to destroy a systems data and registry and is likely part of the ongoing destructive wiper campaign targeting Ukraine.

Lastly, the NCSC in the UK has released guidance for organizations concerned about what impact the recent geopolitical developments would have on them. It is WithSecure's view that the guidance is well balanced and provides excellent communication to senior stakeholders on what is a nuanced and complex topic. It is recommended that the guidance is read in full, and organizations look to implement the advice where it is relevant for them to do so.

WithSecure™ Insight

WithSecure™ expects that reporting and focus on activities relating to the Ukraine-Russia conflict may continue for a while yet. It is important that organizations do not burn out their personnel by being on ultra-heightened alert throughout this entire period and that the sensationalism of the news does not drive security strategies.

It is not clear what effect the Ukraine conflict will have on the activity of Russian threat actors in relation to western entities. In the short term we have observed a clear pattern of destructive activity against Ukrainian targets and some spillover activity on organizations providing services in to Ukrainian CNI. In the medium term this could evolve into a wider range of targets being considered if the conflict escalates or cyber operations are seen as a means to reach a beneficial outcome in the overall conflict. Equally, it is possible that no further escalation could be seen, and the cyber activities remain largely confined directly to the direct conflict itself.

There have been continual warnings issued the US government surrounding the risk that Russian-backed threat actors present to CNI over the last few months and the statement by President Biden continues that theme. Of note, President Biden has also stated “the magnitude of Russia’s cyber capacity is fairly consequential and it’s coming”, perhaps highlighting intelligence that Russia is actively researching or planning an attack on the domestic US CNI. With President Biden also saying, “if Russia pursues cyberattacks against our companies, our critical infrastructure, we are prepared to respond”. These statements point towards the increasing tensions between the US and Russia and highlights how cyber is a potential escalation point and perceived nexus of conflict in the future between Russia and the West.

The more interesting question is what are the long term implications, and whether this sees a long term shift in relations between Russia and the West that changes the norms, objectives and priority of cyber operations between the two sides. Please note that the description of two sides is a conscious simplification for brevity here.

The more important point to consider is that if there is a shift what does this practically mean for the majority of organizations? Well looking at the NCSC guidance we see their view is that “It almost certainly remains the case that nearly all individuals in the UK (and many enterprises) are not going to be targeted by Russian cyber attack”. This is a strong assessment, and one made by an organization that likely has far more visibility and expertise to make such a judgement than the private sector – so one worth weighting accordingly. There are some exceptions to this outlined in the NCSC guidance, and organizations that meet those criteria should be actively considering these impacts. However for everyone else this is a distraction and one they should not allow to alter existing decisions based on their individual threat models.

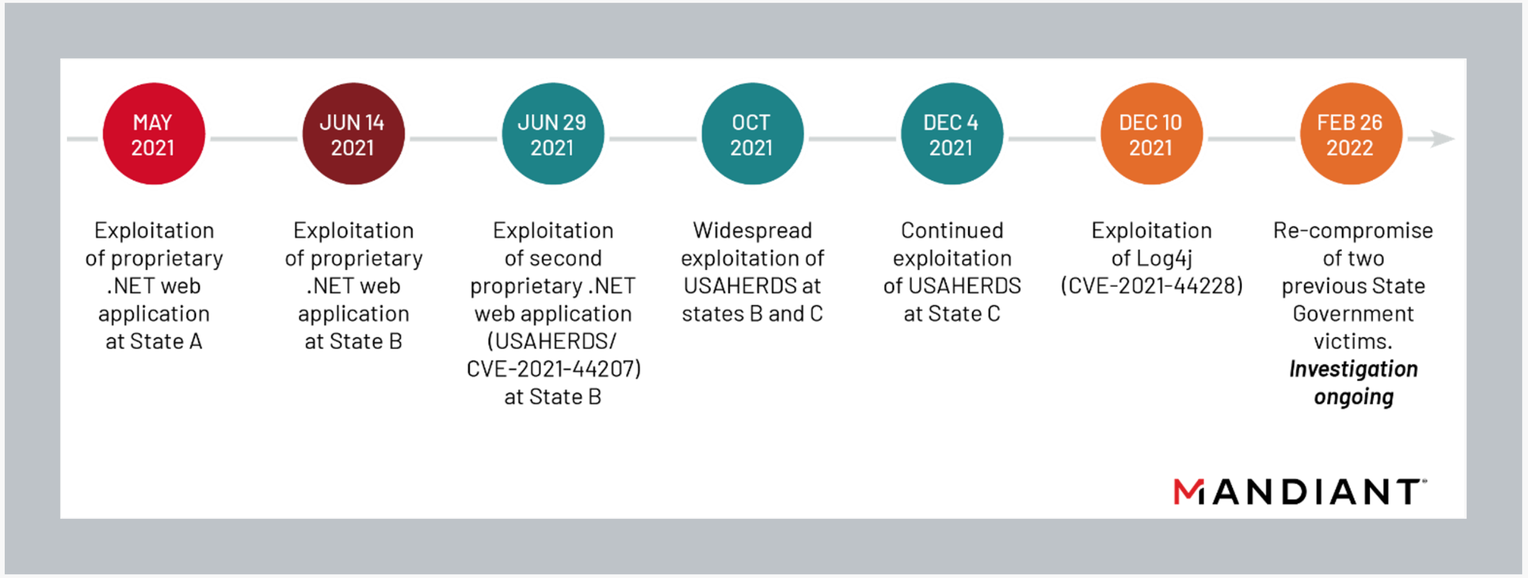
1.3 Chinese backed actor APT41 attacks US government

Researchers from Mandiant have produced a blog post that describes the ongoing activities of APT41, a Chinese-backed threat actor who carries out both cyber espionage activities on behalf of the Chinese Communist Party and financially motivated cybercrime.

APT41 have a history of performing mass scanning activity and opportunistic exploitation of well-known vulnerabilities, but the activity described by Mandiant appears to be highly targeted. Tracked activity between May 2021 and February 2022 evidences an intensive campaign targeting US state governments and resulted in the compromise of at least 6 networks

The techniques being used include .NET deserialization attacks, SQL injection, directory traversal, as well as exploitation of zero-day vulnerabilities such as those present in USAHerds (CVE-2021-44207) and Log4j (CVE-2021-44228). Further tactics, techniques and procedures (TTPs) used by APT41 throughout this campaign include the use of public tools such as YSoSerial.NET, Mimikatz and Cobalt Strike, as well as custom malware and scripts. Mandiant include comprehensive TTP analysis and IOCs within their post.

Mandiant highlight that the goals of APT41 are unclear, but that they been seen to exfiltrate personal identifiable information (PII) from compromised networks, in what is possibly espionage related activity.



WithSecure™ Insight

APT41 are somewhat unusual due to their activity relating to both state-backed espionage as well as personally motivated financial cybercrime, a modus operandi that has resulted in FireEye calling the group “Double Dragon”. The TTPs described by Mandiant in their report clearly demonstrate how APT41 are adept at both custom malware and exploit development, but also willing to add public tools and vulnerability exploits into their toolkit.

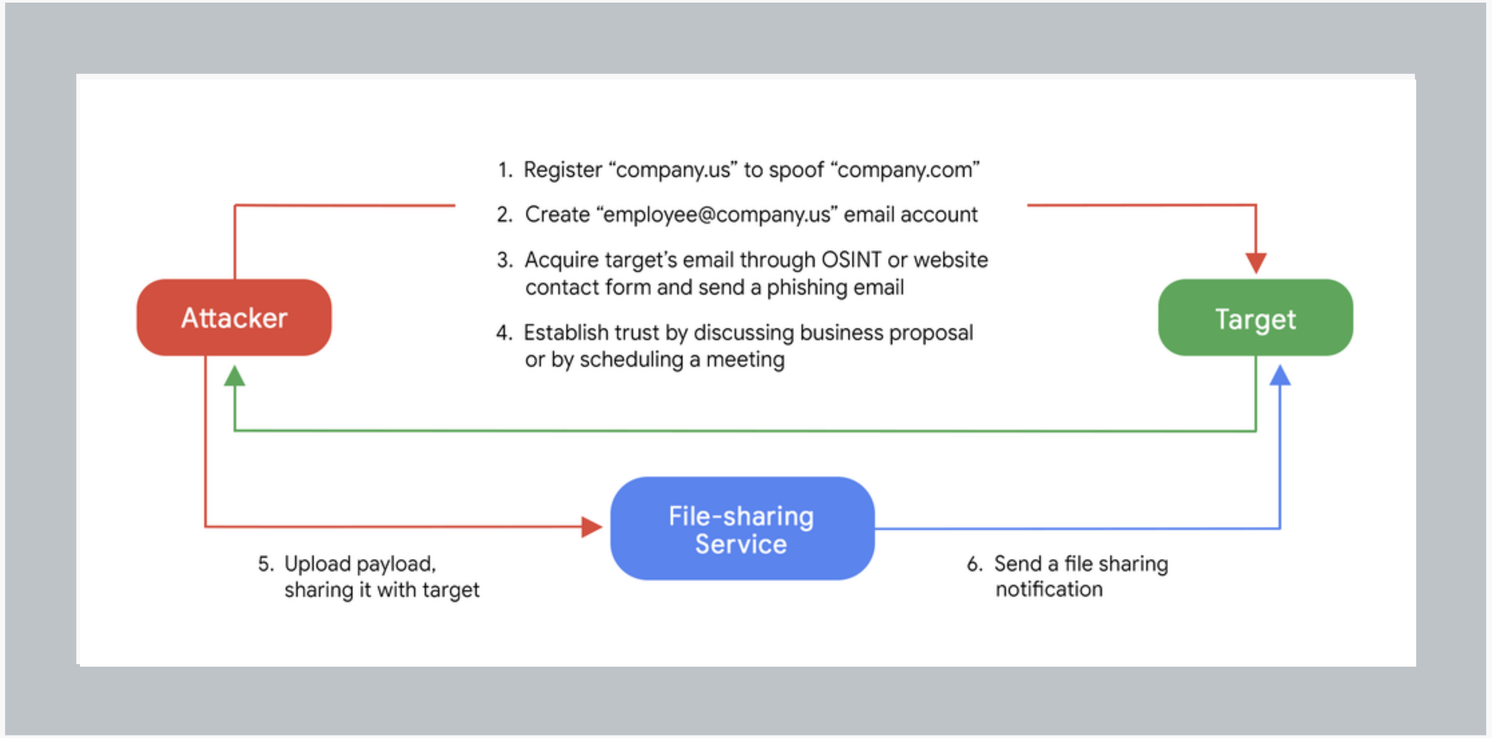
While the motive behind the groups attack on the networks of US state governments is unknown, it demonstrates their capability and resources, highlighting the danger the group pose to similar targets such as international governments, especially those making use of potentially vulnerable web applications. Patching and the management of external attack surface should be a key aspect of any security strategy.

1.4 Initial access broker for Conti uses complex social engineering

Google's Threat Analysis Group (TAG) have released research on an Initial Access Broker (IAB) they are tracking as "Exotic Lily". IAB's are threat actors who specialize in gaining initial access to targets, with the intention to sell that access to other threat groups, who often go on to commit further attacks on the target such as deployment of ransomware.

TAG have linked Exotic Lily to the CONTI and Diavol ransomware groups, suggesting that while they are a distinct entity, that they are serving repeat customers in the form of well-organized cybercriminal groups, and have close relationships with those groups.

Exotic Lily is known to engage in mass phishing, with TAG estimating they are sending over 5,000 emails a day, but in recent times have used tactics involving complex social engineering. These tactics include the creation of pseudo accounts on social media, associated with legitimate companies, and making use of AI generated profile images, as well as the registration of typosquatting domains. They do so, with the intention to engage targets in conversation and building rapport, with the ultimate goal to be the delivery of malware.



Malware is being delivered through legitimate file sharing services such as WeTransfer, TransferNow, TransferXL and OneDrive, with the attackers sending their malware link using the services inbuilt notification service. This method can be difficult for detection and prevention as these services are often trusted by email filtering and security products. Exotic Lily were initially known for exploiting CVE-2021-40444, a vulnerability in Microsoft MSHTML, but are also using malware embedded with loaders such as Bazaar and a custom loader with TAG have dubbed “Bumblebee”, which ultimately results in the delivery of Cobalt Strike.

TAG have included recommendation to improve user protection, which includes better email filtering to provide warnings about emails originating from external file sharing websites, and provide IOCs associated with Exotic Lily.

WithSecure™ Insight

The complex social engineering tactics displayed by Exotic Lily are ordinarily reserved for threat actors associated with state-backed espionage such as Iran’s Tortoiseshell group. This level of effort in order to gain initial access to targets, perhaps highlights how ordinary mass phishing is not providing good results or suggests a specific focus by Exotic Lily on high value targets and specific personnel, who may present low hanging fruit.

Due to the overlap in tactics and techniques with state-backed espionage groups, previously published security advice by the UK Centre for the Protection of National Infrastructure (CPNI) is relevant, and may be of use for frontline staff who may be targeted by Exotic Lily or similar IAB threat actors, who begin to employ similar tactics.

The lines between state-backed threats and cybercriminals are increasingly blurring in terms of tradecraft as the more capable cybercriminals use more advanced capability to achieve their objectives. Therefore, the language we use to describe these different threat actors carries with it bias that can be unhelpful in reporting. The important takeaway for most organizations is that the level of capability deployed by some non-state-backed actors is rising and needs factoring into security strategies.

2 Ransomware: Trends and notable reports

2.1 RURansom targets Russia

Researchers at Trend Micro have analyzed a malware sample called “RURansom”, which appears to be targeting Russia in a response to the invasion of Ukraine. While the malware is similar to many ransomware variants, it is better described as a “wiper” as its encryption is irreversible as the keys are not stored, making decryption impossible. While little is known about the author of the malware, their motivation is clear, with the malware creating a note in each wiped directory stating “…on February 24, President Vladimir Putin declared war on Ukraine. To counter this, I, the creator of RU_Ransom, created this malware to harm Russia”.

2.2 Advisory on AvosLocker

The US Federal Bureau of Investigation (FBI) has published a joint advisory relating to known IOCs associate with the AvosLocker ransomware variant. AvosLocker are a Ransomware-as-a-Service (RaaS) affiliate based group, who are known to target multiple sectors including CNI, by both encrypting and exfiltrating data.

The advisory contains detailed IOCs related to AvosLocker malware samples, as well as known vulnerabilities being exploited by the groups affiliates, with specific mention to Microsoft Exchange vulnerabilities (CVE-2021-26855) and ProxyShell (CVE-2021-31207, CVE-2021-34523, and CVE-2021-34473).

Mitigation advice is also included that is generic and applicable to all ransomware variants, but is relevant and useful nonetheless.

2.3 HermeticRansom can be decrypted

On the 23rd of February a number of Ukrainian entities were targeted by destructive/disruptive malware as part of a cyber-attack designed to coincide with the Russian invasion. One of those attacks involved a ransomware variant called HermeticRansom, which has also been named “PartyTicket” by CrowdStrike.

Analysis carried out by CrowdStrike, describes HermeticRansom as being written in Go and containing a number of coding errors that inhibit its functionality. One of these errors relates to the key used to encrypt files, making it possible to decrypt and recover the data, with CrowdStrike providing a script that can do so.

2.4 Sophos collates their ransomware research

Security company Sophos have released a collation of their research and articles on numerous ransomware groups, titled it the “Ransomware Threat Intelligence Center”. The webpage currently collates data on 37 ransomware groups/variants, dating back to July 2018 and will be updated regularly. It also contains links to Sophos annual threat landscape report, which contains good insights in to the state of the ransomware landscape.

2.5 An analysis of LockBit 2.0

Security researcher Chuong Dong has published in-depth analysis of the LockBit 2.0 ransomware variant on his personal website. LockBit are a prolific RaaS group who advertise for affiliates across hacker forums and have their own .onion leak site, and have recently overtaken CONTI as being the ransomware group to leak the most victim data.

Chuong describes LockBit 2.0 as having “…a hybrid-cryptography scheme of Libsodium’s XSalsa20-Poly1305-Blake2b-Curve25519 and AES-128-CBC to encrypt files. The malware’s configuration is XOR-encrypted and stored in static memory. Like REvil and BlackMatter, LockBit’s child threads use a shared structure to divide the encryption work into multiple states while encrypting a file”. With Chuong concluding that LockBit 2.0 is “definitely the most sophisticated ransomware I have taken a look at”.

2.6 Estonian imprisoned for connection with ransomware and cybercrime

An Estonian national ‘Maksim Berezan’ was arrested in Latvia and later extradited to the United States. Mr Berezan plead guilty to charges of conspiracy to commit wire fraud affecting a financial institution and conspiracy to commit access device fraud and computer intrusion, in relation to his involvement with at least 13 ransomware attacks and a long history with the cyber-criminal underworld. Mr Berezan has been handed a 66 month prison sentence as well as being ordered to pay $36m in restitution.

3 Other notable highlights in brief

3.1 Cyclops Blink expands to Asus routers

Cyclops Blink an advanced botnet associated with the Russian-backed threat actor Sandworm, and previously reported on in last months threat highlight report has reportedly undergone further development and is now targeting Asus routers.

3.2 SharkBot the Android banking trojan

The NCC group have noted a distinct rise in Android malware, and are reporting on a new banking malware called “SharkBot”, which is complex and designed to hijack banking apps to steal money from victims accounts.

3.3 Infostealer distributed via Youtube

The ASEC analysis team have detected an infostealer malware variant that is being distributed through Youtube.

3.4 GhostCringe RAT

The ASEC analysis team have reported on a Gh0st RAT variant named “Gh0stCringe RAT”, which is being distributed through exploitation of vulnerabilities in SMB with the tool ZombieBoy.

3.5 Nigerian authorities arrest suspect wanted by FBI

Nigerian authorities have arrested a criminal wanted by the FBI for offences relating to fraud, money laundering and identity theft.

3.6 Emotet targets tax-season

The threat actors behind Emotet are known to adjust their phishing lures dependent on the time of year and current events, and every year target Americans with phishing emails during the tax reporting period. With some emails containing malicious office documents, and others containing .html files, which can often bypass common email filters.

3.7 An unconvincing Zelenskyy deepfake

A doctored video appearing to show Ukrainian President Volodymyr Zelenskyy appealing to his troops to surrender, has been described by experts as a poor-example of deep-fake technology, but nonetheless damaging, and an example of how deep-fake technology can be used to distribute disinformation.

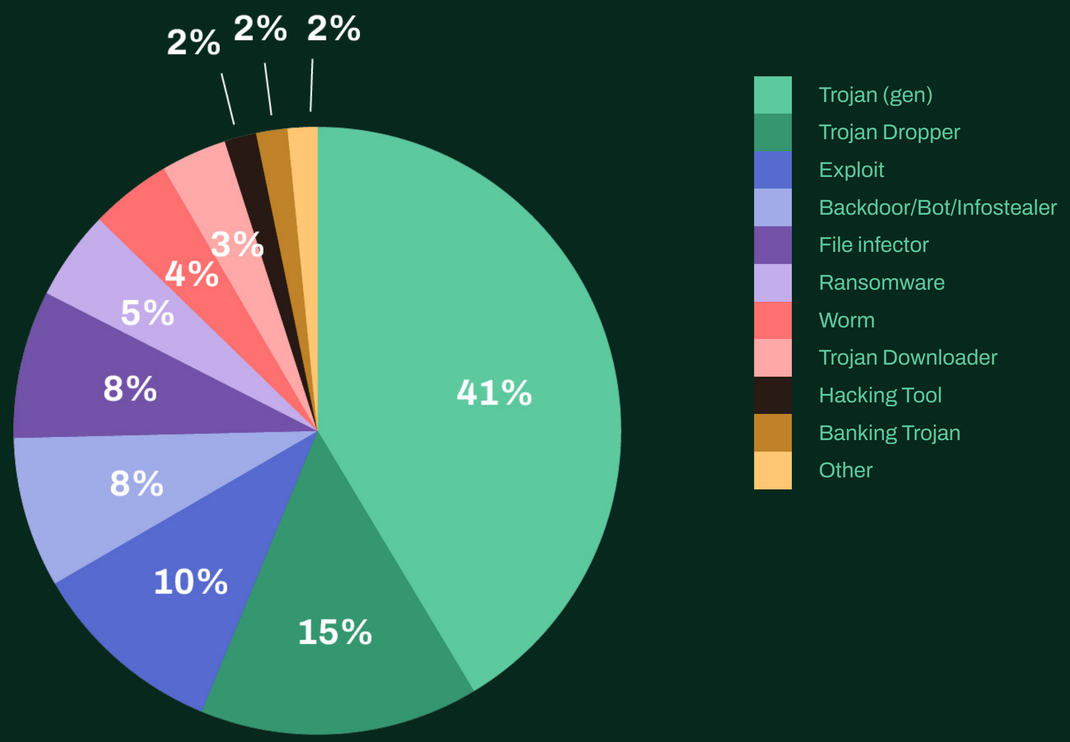
4 Threat data highlights

4.1 Malware types

On the malware front, most detected threats have been various droppers and exploits. These threat types continue to remain prevalent in the first quarter of 2022.

Ransomware has not seen as significant numbers in 2022 as previously anticipated. There may be multiple reasons for this. We have seen cybercriminals deploy exfiltration and extortion tactics without deploying ransomware itself such as in the recent Okta & Microsoft leaks by LAPSUS$ extortion group. Currently most cybercriminals deploy only ransomware or both ransomware and exfiltration tactics. While both have their “benefits” we may see more exfiltration only activity in the future.

The Revil group which dominated ransomware landscape in 2021 has suffered from arrests and destruction of infrastructure and the second biggest contributor in 2021 the CONTI group has suffered from data leaks.



4.2 Exploits

CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker.

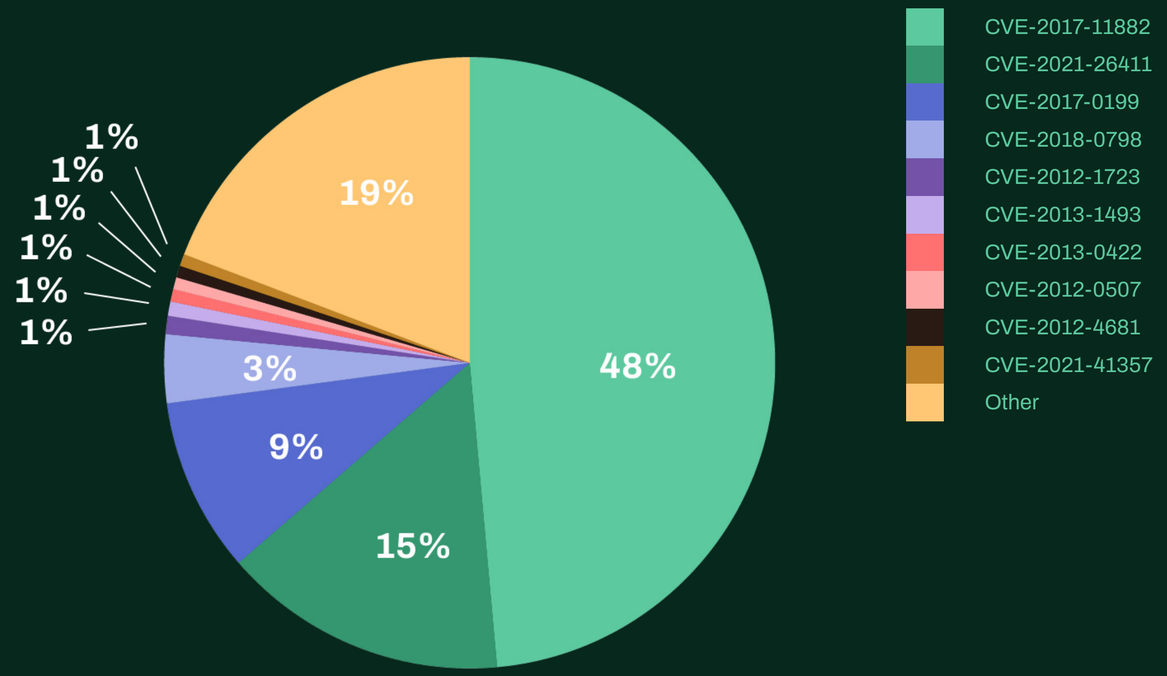
CVE-2021-26411 an internet explorer memory corruption vulnerability which follows at the second place. This vulnerability is exploited by malicious websites.

CVE-2017-0199 is a remote code execution vulnerability in MS Office and Wordpad exploited by a specially crafted file.

In March, CISA added 219 CVEs to the list of vulnerabilities exploited in the wild.

These vulnerabilities affect multiple applications on various operating systems, ranging from internet explorer and edge browser on windows to

wireless access point devices and Elasticsearch.

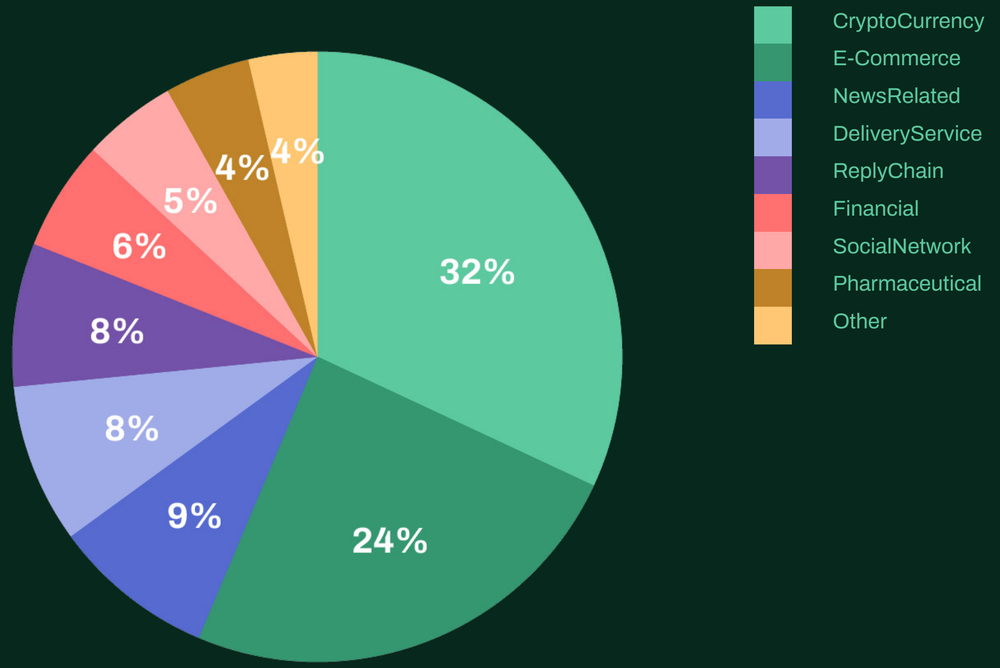


https://www.cisa.gov/known-exploited-vulnerabilities-catalog

4.3 Email threats

Cryptocurrency and e-commerce themes dominate the spam landscape. Last month we highlighted some exploitation attempts of the situation in Ukraine via spam email.

Following on that topic throughout March, we can see an increase in the Ukraine themed emails in general with few bigger volume campaigns. Type of the spam emails are similar to February, unsolicited advertisements and lures with Russia – Ukraine war.



5 WithSecure™ Research Highlights

5.1 A closer look at Flubot's DoH tunneling

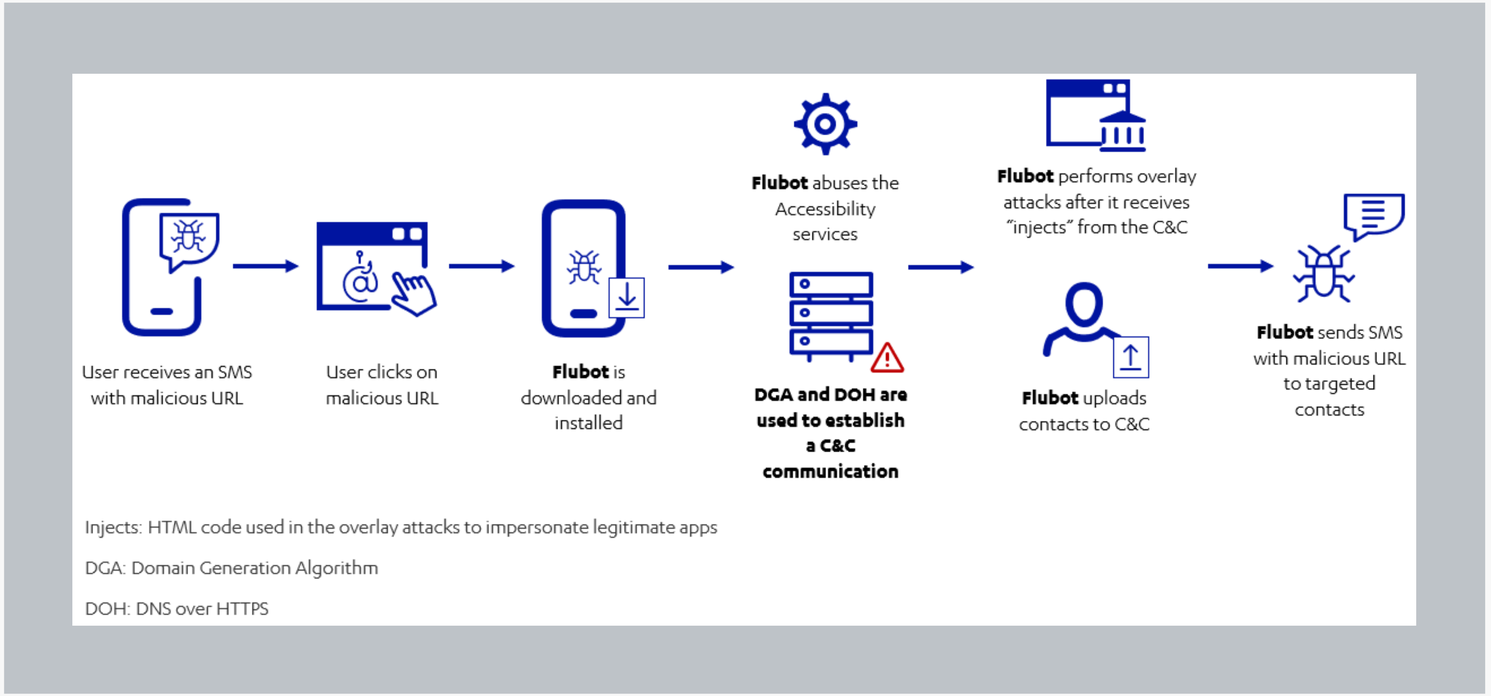
WithSecure™ researcher Catarina de Faria Cristas has published analysis on a sample of Flubot, with a specific focus on its DNS-over-HTTPS (DoH) communication technique.

Flubot is an Android banking trojan, first seen in December 2020, which has gained traction in 2021 and compromised a huge number of devices worldwide. It is capable of stealing information, including credentials, without the user's knowledge and in November 2021 a new Flubot campaign using version 4.9 targeted users in Finland.

The infection vector used to spread Flubot is SMS phishing (smishing), with common lures involving missing parcel deliveries. The malicious link contained within these SMS messages, trigged the download of a Flubot .apk app file.

Flubot's main goal is to perform overlay attacks to steal credentials from banking and cryptocurrency wallet apps as well as one time passwords received by SMS message. But of specific interest in this variant, is the switch to using DoH to communicate with its C2.

DoH has likely been implemented by the threat actors operating Flubot as its requests are encrypted, therefore aggravating detection of suspicious traffic.



Flubot is able to send the following commands to its C2:

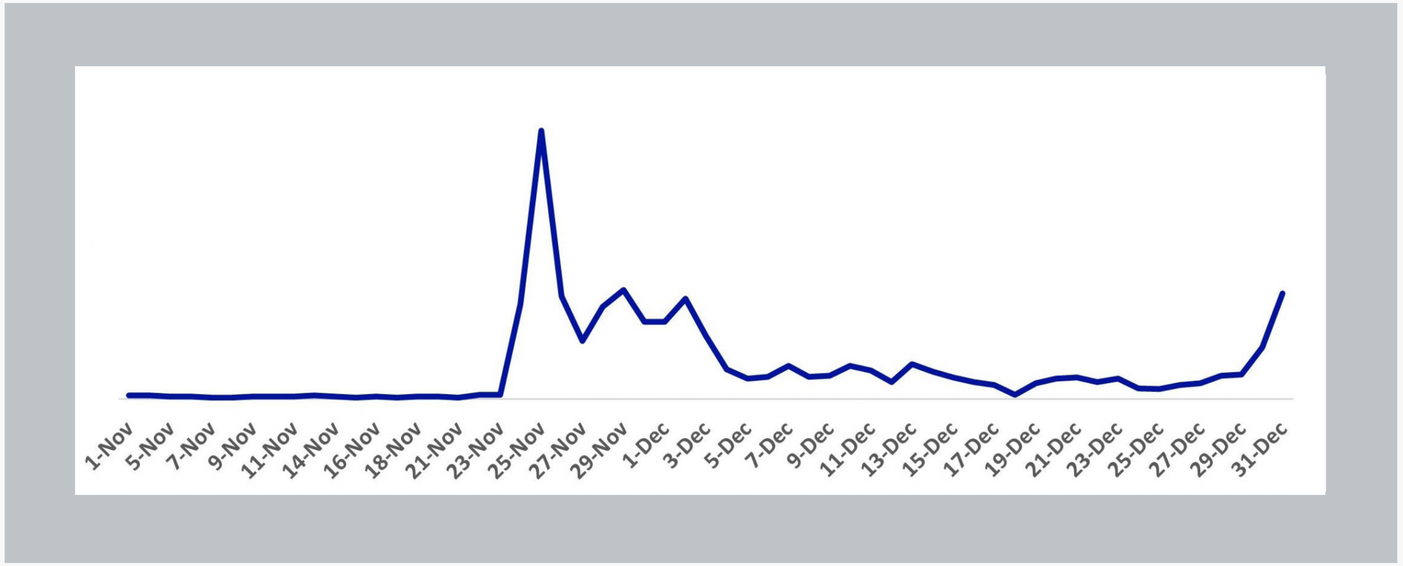
- PREPING,<c2_domain>: Find a working C&C.
- PING,<comma_separated_information>: Send information about the phone.
- LOG,<action>,<information>: Log the malware's behavior and send it to the C&C for debugging purposes.
  <action> is SMS, CONTACTS, NOTIF, SMS_LIST, BLOCK, SOCKS, INTERCEPTING_ERR_NOT_DEF, INTERCEPTING_ERR_NOTIF, INJECT, EXCEPTION, DISABLE_PLAY_PROTECT
  <information> can be optional, it depends on the <action>.
- GET_INJECTS_LIST,<list_package_names_in_phone>: Send the list of the installed apps to determine those that can be targeted by overlay attacks.
- GET_INJECT,<package_name>: Retrieve the inject of a specific app.

Making use of the following DNS providers as part of its communication:

- CloudFlare DNS:
  https[:]//cloudflare-dns[.]com/dns-query?name=<request>&type=TXT
- Google DNS:
  https[:]//dns[.]google/resolve?name=<request>&type=TXT
- NextDNS:
  https[:]//dns[.]nextdns[.]io/resolve?name=<request>&type=TXT
- Alibaba Cloud DNS:
  https[:]//dns[.]alidns[.]com/resolve?name=<request>&type=TXT

As discussed, all of the information exchanged between the malware and the C&C is encrypted. The data sent to the C&C is Base32 encoded and RSA/RC4 encrypted, while the C&C reply is Base64 encoded and RC4 encrypted.

A full in-depth breakdown and analysis of this procedure is include in the blog post.



Who We Are

WithSecure™ 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 & response is 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™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure