Threat Highlight Report

October 2023

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, delivering an overview of this month's cybersecurity news, the changing threat landscape, and relevant advice.

This month, we look at an ongoing phishing campaign impacting Finland, the state of the infostealer market, the fallout following the compromise of Okta, and a new HTTP/2 rapid reset DDoS technique. We also look at the state of the hacktivist landscape, which has been further shaped by on ongoing conflict in Israel.

We continue to track the ransomware landscape, including statistics from known attacks. This month we also include reference to a wider piece of research on the malware Darkgate.

- Ziggy Davies, Intelligence Analyst

1 Monthly highlights

1.1 Finnish Phishing

The Finnish Cyber Security Centre (Kyberturvallisuuskeskus (NCSC)) has received multiple reports relating to a phishing campaign that appears to be targeting Finnish organizations. WithSecure™ is aiding and responding to an incident which appears to be part of the same campaign.

The phishing campaign reportedly involves multiple steps:

- Phishing emails sent from previously compromised legitimate accounts,
- Use of reply-chain phishing, by modifying legitimate secure emails with malicious links,
- Sending these modified emails to other users and organizationsr to attempt to compromise them,
- The phishing sites are advanced and capable of attacker-in-the-middle (AitM) and bypassing of multi-factor authentication (MFA),
- If the attackers are successful, they will quickly use stolen credentials to try and compromise the users Microsoft 365 account,
- The attacker has been seen to reply to emails in Finnish, suggesting a social engineering effort.

WithSecure™ Insight

While these attacks are focused on Finnish organizations and victims, certain indicators overlap with campaigns that also targeted German and Italian organizations earlier in October, suggesting that this is part of a wider campaign.

This attacker appears to be comparatively sophisticated compared to a typical phishing actor, and is utilizing social engineering, efforts to avoid detection by abusing legitimate accounts and services, and AitM techniques.

While the AitM in this case seems similar to use of the known tool/service **EvilProxy**, **EvilGinx** or **EvilGoPhish**, we are not yet in a position to attribute the TTPs to any specific tool/service or known threat actor at this time.

Furthermore, the end goal of the attacker is not yet fully understood, and the campaign appears at this stage, to be limited to phishing and account compromise. This appears to be an ongoing and active campaign and we are conducting research and gathering intelligence to better understand it.

What can you do?

We agree with the Finnish NCSC regarding best practices, and are sharing their mitigation advice as follows:

- *Training and informing personnel,*
- *If you suspect that a message that you have received is fake, don't reply to the message. Instead, check the authenticity of the message in some other way (e.g. phone call, instant message),*
- *If you suspect that an email account has been hacked, check the forwarding rules in the administrator view and the user view,*
- *It is usually not enough to change the passwords of the hacked accounts if the criminals have been able to steal the session cookie,*
- *Check that the attacker hasn't added their own MFA device to the accounts,*
- *Revoke all of the user's access rights momentarily in order to close all open sessions; see https://learn.microsoft.com/fi-fi/azure/active-directory/enterprise-users/users-revoke-access.*

1.2 The state of the infostealer marketplace

Infostealers (a contraction of “information stealers”) have become a common issue in the cybersecurity landscape, and now account for a large proportion of all infections that victims experience.

Upon infection with an infostealer, the malware commonly identifies, gathers, collates and exfiltrates the following information:

- Credentials (saved in browser, but also for specific applications),
- Cookies and tokens, which can be used to login to accounts bypassing MFA,
- Saved form data, such as credit card numbers,
- Personal identifiable information,
- Cryptocurrency recovery “seed phrases”, which can be used to empty wallets,
- Hardware and software information,
- Screenshots,
- Specific files from common directories (desktop, downloads, etc).

The following are popular infostealers currently readily available for hire/purchase on the deep and dark web. This is not an exhaustive list, but representative of the landscape:

Name	Approximate Cost
Vidar	$300 per month
RisePro	$300 per month
Lumma	$250 per month
Rhadamanthys	$250 per month
StealC	$200 per month
Raccoon	$200 per month
Redline	$150 per month
Exela	$20 per month

This table is sorted by approximate cost per month, and there is a clear outlier in the form of newcomer **Exela** stealer. This new infostealer is currently being sold as a MaaS offering for the low-cost of $20, or alternatively $120 for lifetime access. This is by far the cheapest a professionalized infostealer has been offered, and greatly lowers the barrier to cybercrime entry to almost everyone.

WithSecure™ Insight

The widespread adoption and proliferation of infostealer variants is an example of the continued professionalization of cyber-crime. Infostealers are quickly becoming a primary source for breached legitimate credentials, which are then weaponized and abused to commit other cyber-attacks such as the deployment of ransomware or to commit data theft. It has become a highly profitable and widespread business.

At the time of writing, the most prolific infostealer variant is arguably **Redline**, with stealer logs being sold in massive volumes and also freely distributed on certain Telegram channels. This is in part due to its marketing, availability, and functionality, but also its cost ($150 per month) makes it fairly accessible. The newcomer Exela is being advertised at the very low cost of $20 per month, and this is likely to make it a very popular option in the marketplace (if it’s not a scam).

As services such as infostealers become more available and popular, it will undoubtably continue to drive the price lower as groups compete for dominance. At current, a wannabe cyber-criminal can easily and with little knowledge spend their pocket money and begin their credential stealing campaign; this is a worrying issue.

What can you do?

Infostealers are commonly spread through the following vectors:

Malvertising – The abuse of legitimate advertising platforms (Google, Facebook, etc) to direct victims to malicious websites.

SEO poisoning – Similar to malvertising but relies on the manipulation of search engine algorithms to push malicious websites to the top page of search results, driving interaction.

Phishing/Spam – Malware distributed via email remains a common technique and is still a major issue, especially if combined with social engineering pretexts.

Other – Infostealers are commonly associated with “cracked” (pirated) software and video games, and clickbait style YouTube videos on topics such as crypto, video games or software. These vectors are aimed at consumers and the majority of “free logs” seem to originate in this type of compromise.

Organizations can help combat infostealers by raising awareness on and delivering training on these initial access vectors, as well as using security products. WithSecure’s security solutions contain detections for the behaviors exhibited by infostealer malware and these are regularly tuned and updated.

1.3 Okta compromise impacts others

Identity access and management (IAM) company Okta has experienced a breach relating to the compromise of its support case management system. Okta released a statement regarding the breach on the 20th of October, but it appears that the campaign dates back to at least 29th of September. The known timeline is as follows:

September 29th
- 1Password identifies suspicious activity relating to its Okta tenant

October 2nd
- Beyond Trust detects an attack relating to its Okta tenant

October 18th
- Cloudflare investigates a compromise which is traced back to its Okta tenant

October 19th
- 1Password releases a security incident report relating to the attack
- Okta confirms the breach of its support case management system

October 20th
- Beyond Trust releases a blog post regarding the attack
- Cloudflare releases a blog post regarding the attack
- Okta makes a public statement about the breach.

The initial compromise of Okta relates to its support case management system, which is the platform used by Okta to deal with customer support requests and to investigate and resolve issues. Part of this process apparently involves customers uploading HAR files, which are a type of HTTP archive file. Okta states that these files allow it to “*troubleshoot issues by replicating browser activity*”, but that these files can contain “*cookies and session tokens, that malicious actors can use to impersonate valid users*” unless these are removed from the file by customers before upload.

It appears that these HAR files were accessed by the attacker, and the credentials, cookies and session tokens contained within them were abused to access customers' accounts, which led to the incidents at 1Password, Beyond Trust and Cloudflare. All of these third parties appear to have quickly identified the issue, informed Okta and remediated the attacks, ensuring that impact was minimal.

WithSecure™ Insight

Okta has not yet publicly discussed how their support case management system was compromised, but there is speculation that valid credentials of an Okta employee may have been used, suggesting that an Okta employee had been targeted. This is becoming a growing tactic amongst initial access brokers (IAB) who would find Okta a highly attractive target, this is because Okta provide identity and access management services to many other third parties, and compromising them could give access to those customers, allowing a supply chain attack such as that which appears to have occurred in the cases of 1Password, Beyond Trust and Cloudflare. Supply chains pose greatly increase threat surface when trying to secure your organization, and this is an excellent example of how things can go wrong.

Okta has stated that the HAR files involved in this incident are requested to aid the investigation of customer issues. The company's public statement contains a link to the page which includes directions for customers to create a HAR file, which does have a warning message relating to the sanitization of credentials, cookies and session tokens contained in the file:

> ⚠ Sanitize all credentials, cookies, and session tokens in a HAR file before sharing it. HAR files represent a recording of browser activity and may contain sensitive data, including secrets. If not properly sanitized, malicious actors could use the contents of these files to impersonate you. Use caution when creating and sharing HAR files.

It appears that Okta has recently modified this warning, and a previously archived version of the site from June 2023 displays a different version:

> ⚠ HAR files represent recording of browser activity and possibly contain sensitive data, including the content of the pages visited, headers, cookies and other data. While this allows Okta staff to replicate browser activity and troubleshoot issues, malicious actors could use these files to impersonate you. Take care when creating and sharing HAR files.

The sudden change in verbiage used by Okta to describe the risk of HAR files makes it clear that it didn't communicate the risk as clearly as possible in the first instance. It's clear that lessons can be learned from this incident, especially around the complex risks associated with the supply chain, but also in how organizations transparently explain the risk involved in sharing sensitive information such as HAR files.

Okta also played a part in the recent MGM Hotels ransomware incident. While Okta weas not directly targeted, the Okta service used by MGM was allegedly leveraged by the attackers to gain further access to the victim organization.

IAM is an essential service in modern organizations. It helps secure company resources and data, while streamlining access to those systems. In an ideal world IAM makes everything easier and more secure, unfortunately outsourcing this service creates a supply chain. Supply chains bring risk, especially in the case of IAM, which creates a high impact single point of failure. You are essentially relying upon your provider to keep the keys to your castle safe, as are every other customer of that supplier. The recent compromise of Okta highlights what can go wrong if breaches occur, and clearly illustrates why a multi-layered approach to security is vital so that if/when a supply chain is breached, that point of failure is detected at the very next security layer before serious damage can be done.

What can you do?

In Okta's public statement it says that all of the impacted customers have been notified and the stolen session tokens revoked, which should prevent further abuse. This does not help those who have already been compromised, but thankfully Okta has also released known indicators of compromise which can aid threat hunters in identifying malicious activity.

Modern supply chains are complex, and ensuring you mitigate inherent risk with multiple trust relationships and a reliance upon third parties can be very difficult. In this campaign, 1Password, Beyond Trust and Cloudflare were all able to detect malicious activity. Despite no prior knowledge of a compromise at Okta, these companies clearly had good security practices that were able to detect suspicious activity and post-comprise behavior. This highlights the importance of a layered approach regarding security, including best practices, risk management and also the use and active monitoring of security solutions.

1.4 Rapid reset

There is a new technique and exploit being used by threat actors to launch massive, distributed denial of service (DDoS) attacks at a scale that has never been seen before. The technique has been dubbed "Rapid Reset" and involves the exploitation of a vulnerability within the HTTP/2 protocol tracked as CVE-2023-44487, exploiting a feature of HTTP/2 called stream cancellation which an quickly send and cancel request, resulting in DDoS.

Cloudflare, which offer DDoS mitigation services, helped discover the HTTP/2 zero day and detected a number of attacks by an unknown threat actor. Cloudflare's report states:

"*Rapid Reset provides threat actors with a powerful new way to attack victims across the Internet at an order of magnitude larger than anything the Internet has seen before.*"

A common way to measure the scale of DDoS attacks is measuring how many requests per second (RPS) occur, with higher numbers having greater potential for impact. Prior to the implementation of Rapid Reset, the record was 71 million RPS, but Cloudflare reports that since August it has detected 184 different attacks greater in intensity than that record, with one attack measured at 201 million RPS. Both Amazon and Google have reported similar attacks, with Amazon measuring one attack at 155 million RPS, and Google measuring an attack at an astounding 398 million RPS.

Dealing with this type of DDoS is a challenge, but DDoS mitigation providers have been able to successfully thwart them, adapting to the new technique and providing new mitigations to including temporarily blocking IPs that exhibit evidence of exploiting Rapid Reset.

WithSecure™ insight

DDoS has been in the news lately due to the new wave of hacktivist activity associated with the ongoing war in Ukraine and new conflict in Israel, it is ordinarily a low budget, easily accessible tool to (often fairly mildly) impact organizations in order to express negative sentiment. This new type of Rapid Reset-enabled DDoS is far beyond those capabilities and at current is not attributed to a specific threat actor, group or nation-state, but has been carried out by an attacker who has access to a large botnet, suggesting a pre-existing, customizable infrastructure.

The RPS records set by this new DDoS technique are well beyond the attacks that have previously been witnessed and organizations without DDoS mitigation/protections that specifically protect from this type of HTTP/2 attack would likely be greatly impacted and disrupted by such attacks.

What can you do?

At time of writing, there is no reason to suspect a wider campaign involving Rapid Reset and the attacks appear to be testing and probing capabilities, rather than targeted with specific malicious intention. The group behind the **Meris** botnet has claimed the attack on Google, but this has not been confirmed or verified by evidence.

Should this technique be more widely adopted - which is likely due to the presence of freely available exploit code and used by malicious groups such as hacktivists - then impactful attacks are likely. DDoS mitigation/protection services are widely available, and we would recommend you research all the available options and choose one which is capable of dealing with HTTP/2 Rapid Reset attacks.

1.5 Hacktivism

Israel becomes a new hacktivist frontline
The invasion of Ukraine by Russia gave rise to a new wave of hacktivism at a previously unseen level, with over 90 different groups taking part in cyber activity on both sides of the conflict.

It is now apparent that hacktivism has forever shaped the cyber war landscape and is likely to be a part of all future military conflicts and wars and this is certainly the case with the ongoing conflict in Israel, which has given birth to a myriad of actors on both sides of the fighting.

Tracking these groups is an important part of understanding the hacktivist landscape, including gaining knowledge about groups motivations, intentions and capability, and we would like to recognize and commend the excellent work of CyberKnow which regularly provides updates on these groups which has provided us all with valuable insight. Thanks to the group's work we know that there are 111 groups involved in the Israel conflict, with 17 being pro-Israel, and 94 being anti-Israel. Much like the Russia/Ukraine activity, the groups operating in response to the ongoing conflict in Israel are mainly relying upon DDoS as a weapon, but some groups are more impactful and engaging in hack and leak attacks, and potentially worrying activity by **Stucx Team** impacting SCADA/ICS systems.

Guatemala government targeted
The hacktivist collective **Anonymous** has claimed responsibility for DDoS activity which impacted government websites in Guatemala. Anonymous claims that the attacks are in support of recent protests by people calling for the resignation of the attorney general Consuelo Porras, and other government officials.

Anonymous has always acted on issues which it perceives to be undemocratic or related to the unfair treatment of communities and this attack appears to be in-line with the group's values.

Red Cross guidelines

Legal advisors related to the Red Cross have recently published 8 rules which they believe should be followed by civilian hackers (hacktivists), they are as follows:

1. Do not direct cyber-attacks against civilian objects,
2. Do not use malware or other tools or techniques that spread automatically and damage military objectives and civilian objects indiscriminately,
3. When planning a cyber-attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians,
4. Do not conduct any cyber operation against medical and humanitarian facilities,
5. Do not conduct any cyber-attack against objects indispensable to the survival of the population or that can release dangerous forces,
6. Do not make threats of violence to spread terror among the civilian population,
7. Do not incite violations of international humanitarian law,
8. Comply with these rules even if the enemy does not.

It is clear from these guidelines that the focus is on limiting the impact of attacks, so that innocent people do not suffer. This is an honorable pursuit, but is unfortunately wishful thinking for two main reasons.

- These groups are often unmanaged and getting them to conform to a set of rules is unlikely,
- The main tool these groups utilize is DDoS, and this is practically useless against hardened military and governmental systems, and is therefore mainly used to target private and public systems which present lower hanging fruit. Hitting these systems likely contravenes many of the rules mentioned.

And to further confirm our thoughts, a pro-Ukrainian hacktivist group subsequently defaced the Russian website of the Red Cross with a clear message "*there are no rules in war...*".

2 Ransomware: Trends and notable reports

The following data is limited to multi-point of extortion groups who are operating a leak site which is parseable. The data was captured between 1st October-31st October 2023.

This month has seen a significant drop (-28%) in activity compared to September. This is attributable to significantly reduced numbers coming from **3am**, **Blackbyte**, **Cactus**, **Everest**, **RagnarLocker** and **Trigona**.

This month has also only had one newcomer: **Hunters International**, an apparent reincarnation of **Hive**.

Group	Victims	Percentage	Change From Last Month
0mega	2	1%	Returned
3am	2	1%	-80 %
8Base	20	5%	5 %
Abyss Data*	1	<1%	-50 %
Akira	12	3%	33 %
Alphv (BlackCat)	33	8%	-42 %
Arvin Club	6	2%	500 %
BianLian	14	4%	-42 %
BlackBasta	18	5%	Returned
Blackbyte	1	<1%	-83 %
Black Suit	2	1%	100 %
Cactus	5	1%	-85 %
Clop (Torrents)*	1	<1%	Returned
Cuba	3	1%	Returned
Donut Leaks	3	1%	No Change
Everest	1	<1%	-80 %
Hunters International	2	1%	New
INC Ransom	9	2%	-18 %
Knight	6	2%	-45 %
LockBit	63	16%	-26 %
Lorenz	2	1%	No Change
Mallox	4	1%	300 %
Medusa	19	5%	64 %
Money Message	4	1%	No Change
Monti	8	2%	100 %
NoEscape	65	15%	195 %
Play	40	10%	48 %
Qilin	5	1%	25 %
RagnarLocker	5	1%	-64 %
Ransomed	27	7%	-34 %
RansomExx	1	<1%	Returned
Ransomhouse	2	1%	-50 %
Ransomware Blog	3	1%	Returned
Rhysida	5	1%	-29 %
Snatch	5	1%	25 %
Trigona	3	1%	-73 %
Total	**402**		**-28%**

2.1 Need for speed

A recent report by Secureworks states that ransomware dwell times has fallen to less than 24 hours.

Dwell time is the amount of time between an attacker gaining initial access and undertaking their final objective, and in the case of ransomware attacks is the time between access and the detonation of an encryption locker.

The report states that over the last 12 months dwell time has reduced from an average 4.5 days to less than 24 hours, and this is something that has been seen across the cyber security sector. We believe this observation is valid, but note that many cases investigated by WithSecure™ do still involve dwell times that occur over days, and that rapid attacks are limited.

2.2 Hello Kitty code leak

A user of the underground hacker forum XSS called **kapuchin0** has leaked the source code for ransomware variant **HelloKitty**. The malware has subsequently been uploaded to malware repositories on GitHub, allowing researchers (and copycats) to analyze the lockers functionality.

This is a double edged sword, because while access to the malware gives defenders the opportunity to learn and create better defenses, it also provides wannabe ransomware actors access to high quality code that can be modified to create their own locker and launch their own campaign. The leaks of **Babuk**, **Conti** and **LockBit** code have taught us that copycats are likely to follow leaks, and we are likely to see utilization of HelloKitty ransomware by some groups moving forward.

2.3 Black “Munchkin” Cat

Alphv (aka BlackCat) are a ransomware titan which regularly updates its attack tooling and techniques to become more efficient, effective and able to evade defenders. The group’s most recent variant dubbed **Sphynx** has gained a new tool called **Munchkin** (the criminals at **Alphv** clearly enjoy cats), which is designed to target remote machines.

Reports state that Munchkin is being delivered via ISO file, which is then loaded into a Virtual Box instance, and consists of a custom version of Alpine OS to act as a platform for Alphv’s attack. The focus is on targeting remote machines, and SMB/CIFS, but bringing your own custom VM loaded with malicious scripts is also a useful way to try and evade defenses, which are likely installed on the host system.

2.4 Is it legal to pay a ransom?

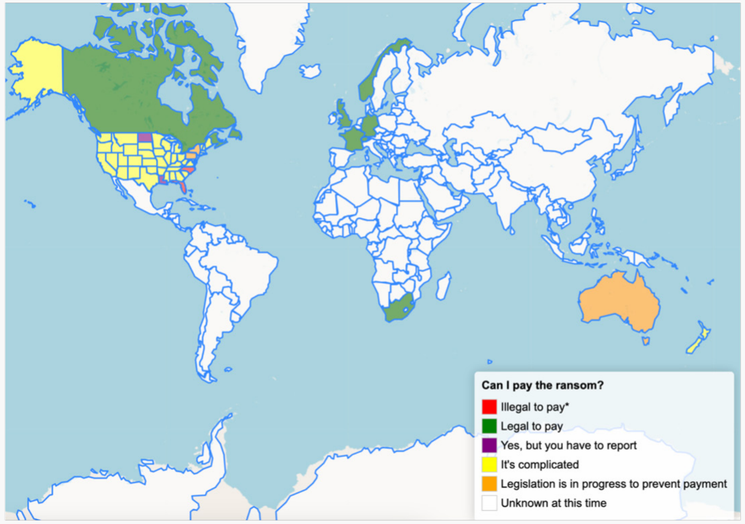
Paying ransoms is always a contentious issue, and we discussed the difficulties in trying to enforce this in last month’s Threat Highlight Report. To review, we appreciate that paying ransoms isn’t an ideal solution when considering the macro problem of ransomware because…

- paying encourages further attacks,
- paying does not necessarily mean you will get your data back,
- paying funds criminal groups, allowing them to invest in the professionalization of cyber-crime.

We also appreciate it’s not necessarily that straightforward because…

- ransomware can greatly impact your organization and reputation,
- you may face pressure to pay a ransom in an effort to restore critical services,
- you may face pressure to pay a ransom in order to prevent the leak of sensitive data.

But legislators across the globe are looking at the issue of ransomware, and wondering if making ransom payments illegal will help combat the problem and provide a clearer process for dealing with attacks and ransom demands. This is the case for the US States of Florida and North Carolina, which have banned the payment of ransoms involving attacks on state/government entities. The government of Australia and other US states are considering similar legislation. It's important to note that these laws don't necessarily apply to private organizations, but making guidance on paying ransoms is likely a good step in limiting criminal's profits. The following is an interactive map created by Ryan Kovar which shows the state of legality in regard to paying ransomware demands:



2.5 Goodbye Trigona and Ragnar Locker

The Trigona ransomware group have been infiltrated and shut down thanks to the actions of the hacktivist group **Ukrainian Cyber Alliance** (UCA). The **UCA** was allegedly able to infiltrate Trigona's infrastructure, exfiltrating all of their data, source code, hot crypto wallets and records, before shutting down the group's leak site. A statement by the UCA states that if any decryption keys for victims are found within the data, then these will be shared to aid recovery.

A joint operation by law enforcement and Europol has shut down the operation of ransomware group Ragnar Locker, with the groups alleged developer/leader being arrested in France, and others being arrested / interviewed in Czechia, Spain and Latvia. Ragnar Locker was responsible for at least 31 attacks in 2023, and this positive action is welcome news.

3 Other notable highlights in brief

3.1 DPRK (still) using job adverts

The DPRK's **Lazarus Group** are well known to utilize social engineering and a network of fake profiles across social media websites to aid their campaigns. A recent report has highlighted a campaign by Lazarus involving the following elements:

- Targets were contacted via LinkedIn, by a "recruiter" who sent them a trojanized coding challenge,
- three different payloads were possible,
- one of which is the backdoor **LightlessCan**.

The goal for this campaign was to conduct cyber espionage against a Spanish aerospace company, likely to steal secrets and the pursuit of financial gain.

3.2 Badbox and PeachPit

The **BADBOX** campaign is a complex fraud scheme that involves malware being deployed on physical off-brand Android devices along the supply chain process in China. This malware, called **Triada**, then infects other devices.

One branch of the BADBOX scheme is the **PEACHPIT** ad fraud botnet. PEACHPIT consists of a conglomerate of apps that were installed more than 15 million times before being taken down. HUMAN, a cybersecurity company, was able to identify and disrupt the PEACHPIT botnet.

The BADBOX campaign is significant because it shows how sophisticated attackers are becoming. They are able to deploy malware on devices before they are even sold to consumers. This makes it very difficult for consumers to protect themselves.

3.3 Zero Signal 0-days identified

During October, persistent rumors were spreading that there was a 0-day vulnerability in Signal's link preview functionality. These rumors allegedly came from US Government sources. CISA stated it had no information on a 0-day targeting Signal, and Signal also stated that after investigating, it was not only unable to identify any security flaws in that functionality, but that it had not received any information or evidence to suggest the vulnerability was real. As such, it appears that the entire story was simply a viral set of rumors.

3.4 Etherhiding malicious code in a cryptocurrency blockchain

Researchers at Guardio discovered that a previously reported campaign which modified compromised WordPress sites to push infostealers including RedLine, Amadey, and Lumma had implemented a new method of hosting part of their malicious payload.

Previously, the malicious JavaScript code that was inserted into the compromised sites was hosted on Cloudflare, however this was taken down by Cloudflare themselves. In response, the attackers uploaded a snippet of obfuscated code into the Binance Smart Chain, a Binance owned "smart contract" focused blockchain. As such, all they had to do was insert a reference to the BSC hosted smart contract into the compromised WordPress sites, which will download the malicious code, de-obfuscate and execute it. The code in the smart contract is relatively prosaic, in that it references another, second-stage malicious domain, but every time that second-stage domain is burnt and needs to be replaced, the attacker simply updates the smart contract to reference a new domain.

So far the attacker has updated the domain in the smart contract at least 30 times. Due to the nature of blockchains, even though BSC is owned and operated by Binance, they cannot "remove" or block this malicious reference. While this is just one instance of such behavior, if this method turns out to be successful for this attacker, others will surely follow.

3.5 Qakbot customers ride again with RansomKnight

In a recent blog post, Talos researchers detailed how they were tracking the behavior of various clusters of Qakbot actors at the time of the FBI lead takedown of Qakbot C2 infrastructure.

Qakbot was a MaaS used my many different operators/ groups. The researchers were tracking certain clusters of Qakbot activity by the metadata of malicious LNK files used in the campaigns. After the Qakbot takedown however, Talos observed that malicious LNK files with the same Drive serial number metadata were being used to distribute RansomKnight ransomware, along with the Remcos backdoor. The use of the same Drive serial number means it is very likely these malicious files were created on the same computer as the Qakbot files were.

The filenames of the LNK files imply that they relate to urgent financial matters, which suggests they are being distributed via phishing, as were the previous Qakbot campaigns. This suggests that when Qakbot C2 servers were taken down, this particular group simply changed its phishing campaign payload from Qakbot to RansomKnight.

It remains to be seen whether the takedown of Qakbot will have any greater impact than forcing actors to change their payload, which QakBot actors so far heavily relying upon alternative offerings such as Darkgate, as discussed in last month's Threat Highlight Report.

4 Threat data highlights

4.1 Vulnerabilities & Exploits

Vulnerabilities of note

Cisco IOS XE Web GUI
CVE-2023-20198

On Monday 16 October 2023 Cisco announced that their IOS XE Web UI contained a 0-day privilege escalation vulnerability CVE-2023-20198 with a CVSS score of 10.

The advisory stated that the 0-day had been under active exploitation by an unknown actor since at least 18 September 2023 who was exploiting Cisco devices where the Web GUI was enabled and exposed to the internet.

Cisco stated the actor used this vulnerability along with either CVE-2021-1435, or another apparent 0-day which is as yet unknown, to install implants which enable arbitrary remote command execution.

Public reporting states that researchers have identified over 40,000 Internet connected Cisco devices which have been implanted by one or more threat actors.

CVE-2023-20198 applies to both virtual and hardware Cisco devices.

With over 40,000 implanted devices this may not seem like a targeted campaign, however it is unknown how many of those devices have received follow on actions from the attacker, if any have. It is common practice for threat actors including APTs to perform mass exploitation of any vulnerable devices, while only actually taking additional actions on specific targets to achieve their goals.

What is significant here is the scale of this campaign, and the fact that an actor has used two 0-days in Cisco IOS devices, which make up a significant percentage of enterprise network infrastructure.

Of additional concern in this case is just how unclear the situation has been. Cisco originally announced one zero-day had been used, alongside CVE-2021-1435, but also stated that the attacks were successful even when the CVE-2021-1435 was patched. This could have meant that the patch was flawed, or that there was another, unknown 0-day being used. Within a week, Cisco announced that CVE-2021-1435 was not associated with the campaign, instead another previously unknown 0-day, CVE-2023-20273 had been used.

Citrix Bleed
CVE-2023-4966

Exploits exists for a vulnerability dubbed “Citrix Bleed” (CVE-2023-4966), which allows attackers to steal authentication session cookies from vulnerable Citrix NetScaler ADC and Gateway appliances.

Citrix patched the vulnerability in October 2023, but attackers have been able to exploit it since late August 2023 and the scale of this attacks has exponentially increased since that time. It is highly likely that session cookies/tokens stolen in these attacks are being sold for the intention of gaining initial access. It’s therefore vital that all users of Citrix NetScaler ADC and Gateway devices install the latest security patch as soon as practicable and after upgrading, users should end all sessions in case they have been compromised and monitor access logs for any suspicious activity.

Atlassian Confluence
CVE-2023-22515

This vulnerability in Atlassian Confluence Data Center and Server allows attackers to create unauthorized administrator accounts and gain access to Confluence instances. It has been exploited by attackers, and is still under attack with Greynoise tracking a recent surge in exploitation which likely means that most vulnerable instances have now been compromised.

Atlassian Confluence
CVE-2023-22518

Atlassian has issued an advisory warning users of Confluence to "take immediate action", in order to fix a vulnerability in the collaboration tool. This vulnerability is tracked as CVE-2023-22518 and the advisory states it scores a CVSS score of 9.1, making it a CRITICAL vulnerability.

Atlassian describes the vulnerability as an "Improper Authorization Vulnerability in Confluence Data Center and Confluence Server", but hse not provided any specifics regarding the nature of potential exploit or potential impact.

Atlassian has released fixed versions and urge users to update immediately.

This vulnerability comes on the back of another (as above) recent CRITICAL Confluence vulnerability (CVE-2023-22515) which has been widely exploited by several different attackers, including ransomware initial access brokers (IABs).

F5 BIG-IP
CVE-2023-46747

Attackers are actively exploiting this vulnerability as part of an attack chain with CVE-2023-46748, allowing them to execute commands on vulnerable BIG-IP instances. Exploitation of this is trivial thanks to publicly available exploit code.

F5 has released fixed/updated versions of BIG-IP to resolve the matter, along with IOCs to aid hunting by defenders.

Curl
CVE-2023-38546

Initially the vulnerability in curl/libcurl was announced with commentary that it was probably the worst security flaw in Curl in a long time and that the patch release cycle was being cut short, causing some alarm within the security community.

On balance this alarm was justified due to aforementioned commentary and the fact that significant bugs in software libraries are notoriously difficult to detect if and where they are used in enterprise software packages. These issues get more serious still where they are present in applications that are internet accessible - rather expected of libcurl. This was the case for Log4J, which was so severe as it presented such a broad attack surface.

In this case, the vuln seems to be related to SOCKS5 local DNS resolution where hostname > 255 chars. This appears to limit the attack surface to implementations where SOCKS is in use, and for an attacker to control the hostname or redirect of a page (although this may be achieved with a 0 click method using prefetch functionality in applications that uses CURL). It does make for a bunch of interesting exploit scenarios, but as far as we can currently tell - nothing internet melting, and a far cry from the tagline 'curlmageddon' that some had assigned to the vulnerability.

JetBrains TeamCity
CVE-2023-42793

Microsoft has reported that two distinct DPRK groups are actively exploiting this vulnerability, in a campaign which appears to focus on cyber espionage and data theft. Unfortunately, thanks to the ease of identification and exploitation, it is highly likely that most vulnerable instances have already been targeted. Microsoft's report details IOCs and hunting queries that may aid defenders in identify compromise of vulnerable TeamCity instances, and JetBrains has provided a patch that fixes the issue.

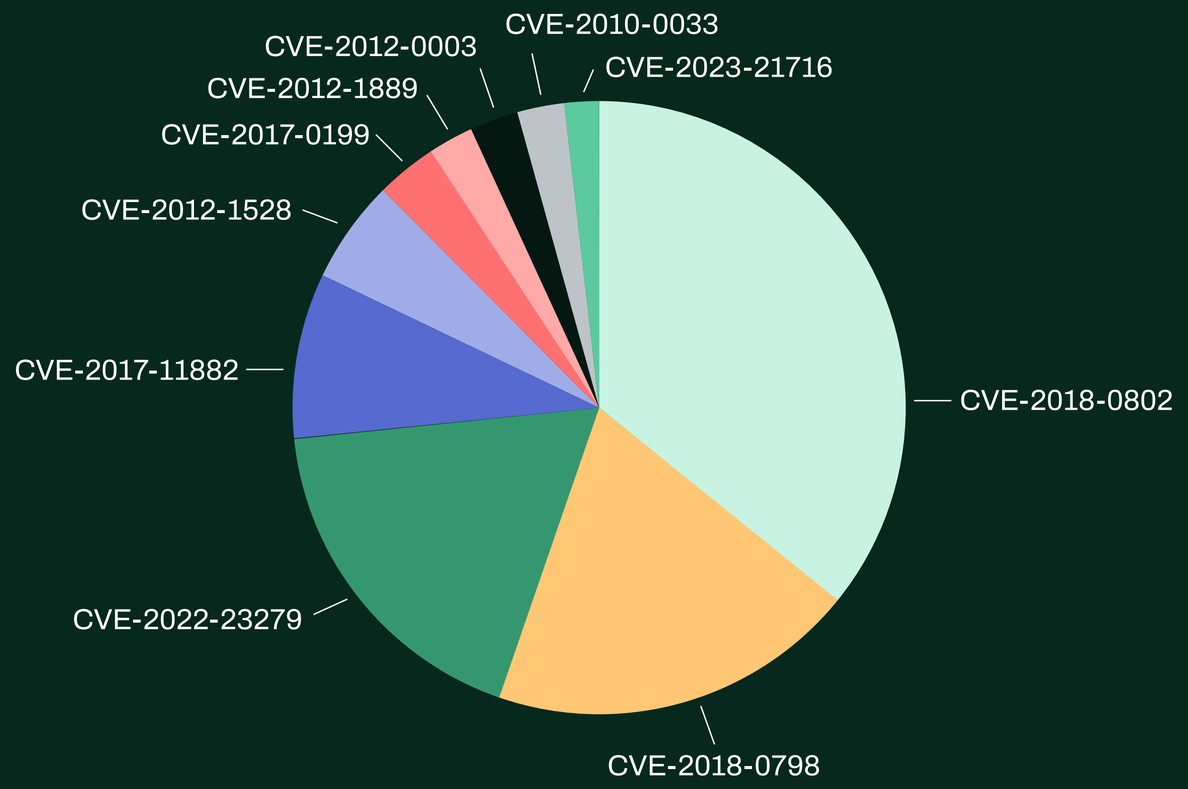
WinRAR
CVE-2023-38831

We discussed two vulnerabilities in WinRAR in August's Threat Highlight Report, and there are reports that the Russian adversary **Fancy Bear (APT28)** *(and others) have been exploiting CVE-2023-38831 as part of their attacks. There are new versions of WinRAR available which fix the issue, but these rely upon patch management as WinRAR does not feature auto-updates, resulting in many instances still being vulnerable.*

What have we seen?

This data is taken from WithSecure's EPP (EndPoint Protection) telemetry, and relates to detections of LOCAL vulnerabilities, typically delivered as part of malware. Remote/network exploitation of edge services are not in scope.

The top 10 vulnerabilities witnessed in our EPP telemetry this month are as follows:



Of note is a new entry by CVE-2022-23279,
an escalation or privilege vulnerability in Windows ALPC.

What vulnerabilities are being newly exploited?

The following are additions to CISA's known exploited vulnerability catalog. Five have received a CVSS rating of "CRITICAL".

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-42793	JetBrains TeamCity	Critical	"JetBrains TeamCity contains an authentication bypass vulnerability that allows for remote code execution on TeamCity Server."
CVE-2023-22515	Atlassian Confluence	Critical	"Atlassian Confluence Data Center and Server contains a broken access control vulnerability that allows an attacker to create unauthorized Confluence administrator accounts and access Confluence."
CVE-2023-40044	Progress WS_FTP Server	Critical	"Progress WS_FTP Server contains a deserialization of untrusted data vulnerability in the Ad Hoc Transfer module that allows an authenticated attacker to execute remote commands on the underlying operating system."
CVE-2023-20198	Cisco IOS XE Web UI	Critical	"Cisco IOS XE Web UI contains a privilege escalation vulnerability in the web user interface that could allow a remote, unauthenticated attacker to create an account with privilege level 15 access. The attacker can then use that account to gain control of the affected device."
CVE-2023-4966	Citrix NetScaler ADC & Gateway	Critical	"Citrix NetScaler ADC and NetScaler Gateway contain a buffer overflow vulnerability that allows for sensitive information disclosure when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server."
CVE-2023-5217	Google Chrome Libvpx	High	"Google Chrome libvpx contains a heap buffer overflow vulnerability in vp8 encoding that allows a remote attacker to potentially exploit heap corruption via a crafted HTML page."
CVE-2023-28229	Microsoft CNG Key Isolation Service	High	"Microsoft Windows Cryptographic Next Generation (CNG) Key Isolation Service contains an unspecified vulnerability that allows an attacker to gain specific limited SYSTEM privileges."
CVE-2023-42824	Apple iOS, iPadOS	High	Apple iOS and iPadOS contain an unspecified vulnerability that allows for local privilege escalation.
CVE-2023-21608	Adobe Acrobat & Reader	High	"Adobe Acrobat and Reader contains a use-after-free vulnerability that allows for code execution in the context of the current user."
CVE-2023-44487	IETF HTTP/2	High	HTTP/2 contains a rapid reset vulnerability that allows for a distributed denial-of-service attack (DDoS).
CVE-2023-20273	Cisco IOS XE Web UI	High	"Cisco IOS XE contains a command injection vulnerability in the web user interface. When chained with CVE-2023-20198, the attacker can leverage the new local user to elevate privilege to root and write the implant to the file system. Cisco identified CVE-2023-20273 as the vulnerability exploited to deploy the implant. CVE-2021-1435, previously associated with the exploitation events, is no longer believed to be related to this activity."
CVE-2023-4211	Arm Mali GPU Kernal Driver	Medium	"Arm Mali GPU Kernel Driver contains a use-after-free vulnerability that allows a local, non-privileged user to make improper GPU memory processing operations to gain access to already freed memory."
CVE-2023-20109	Cisco IOS XE	Medium	"Cisco IOS and IOS XE contain an out-of-bounds write vulnerability in the Group Encrypted Transport VPN (GET VPN) feature that could allow an authenticated, remote attacker who has administrative control of either a group member or a key server to execute malicious code or cause a device to crash."
CVE-2023-41763	Microsoft Skype	Medium	Microsoft Skype for Business contains an unspecified vulnerability that allows for privilege escalation.
CVE-2023-36563	Microsoft WordPad	Medium	Microsoft WordPad contains an unspecified vulnerability that allows for information disclosure.
CVE-2023-5631	Roundcube Webmail	Medium	"Roundcube Webmail contains a persistent cross-site scripting (XSS) vulnerability that allows a remote attacker to run malicious JavaScript code."

5 Research highlights

5.1 DarkGate

WithSecure™ Cyber Threat Intelligence published research into a financially motivated cybercrime actor that is using multiple malware families, including the Darkgate MaaS to target digital marketing professionals.

Analysis of the targeting methods and lure documents was able to confidently identify that certain Darkgate campaigns are being carried out by the same Vietnamese threat actor cluster using Ducktail and Duckport. The specific purpose of this threat grouping appears to be to hijack Facebook/Meta business accounts.

By analyzing the DarkGate campaigns attributed to this threat actor, additional campaigns which used multiple different malware families were also identified, often through non-technical analysis of the lure files used.

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.

Our latest reports: Threat-Research