Threat Landscape Update

February 2024

WITH secure

Contents

Foreword

The Ivanti ConnectSecure mass exploitation incidents of January continued into February, along with yet another zero-day announcement by Ivanti. There was also a second set of mass exploitation incidents targeting vulnerabilities in ConnectWise ScreenConnect, which the WithSecure Threat Intelligence team published research on. The takedown of Lockbit by international law enforcement's Operation Cronos this month was heavily reported on in the media, though the true impact of the operation remains to be seen.

Ransomware attacks continued, though multiple different year end summaries provided different opinions and statistics regarding the state of the ransomware sector. Several reports cover the use of Machine Learning and LLMs for malicious activity such as fraud, and even a research project which successfully trained LLMs to perform autonomous hacking.

- Stephen Robinson, Senior Threat Intelligence Analyst, WithSecure

1 Monthly highlights

1.1 Mass exploitation of ConnectWise ScreenConnect

On the 20th of February, CVE-2024-1708, a maximum severity vulnerability in ConnectWise ScreenConnect was published. A patch was released at the same time, and security researchers soon found that the vulnerability was not only extremely severe, but also trivial to exploit. By the 21st of February proof of concept code was published, and the simplicity of the exploit gave even low skilled attackers the ability to remotely gain administrative access to a ScreenConnect server. ScreenConnect is a client/server based Remote Monitoring and Management (RMM) tool which is extensively used in enterprise environments, particularly by Managed Service Providers (MSPs) who can use it to manage devices across multiple customer estates through a single server. At the time the vulnerability and patch were published there were more than 5-10,000 ScreenConnect servers visible to the Internet. Combine this with the fact that this is an enterprise solution where each server can manage up to 150,000 clients and the potentially affected install base is huge. It was not long until exploitation began with multiple groups and payloads reported, including multiple ransomware variants. Exploitation was first observed by WithSecure Detection and Response on 22nd of February, and on the 24th WithSecure Threat Intelligence published details of a ScreenConnect mass exploitation campaign by a malicious actor, which we were then able to link to multiple previous mass exploitation campaigns over the last 6 months.

1.2 Lockbit takedown

Also on the 20th of February, an International Law Enforcement Agency (LEA) action codenamed Operation Cronos posted a seizure notice in place of the Lockbit leak site. In a deeply enjoyable display of irony and humor, the format of the Lockbit leak site was itself used to taunt Lockbit and to present information about the successes of the LEA operation, and information gained about Lockbit operations. LEA also gained access to the affiliate communications/control panel and were able to leave messages threatening Lockbit affiliates. While the full extent of LEA's access to Lockbit is not presently public knowledge, what is known is that the operation seized several hundred cryptocurrency wallets holding ~$120 million, took control of 34 Lockbit servers, retrieved 1,000 decryption keys for Lockbit victims, and at the same time coordinated the arrest of two Lockbit associated hackers in Ukraine and Poland, respectively. In the week following the operation the Lockbit leak site was brought back online, along with a long message that attempted to downplay the effects of the take down. LEA also offered a $15 million reward for information leading to the arrest of senior Lockbit members, which does at least imply that they do not currently have such information.

At this point LEA and Lockbit have each made different statements about the breadth and impact of the takedown, and they are each trying to win a PR war to either kill or keep alive the Lockbit brand. Who will win at this time is unclear, though some commentators have noted that the immediate surge in claimed Lockbit activity after the takedown is similar to what happened after the Conti takedown. In that case sufficient damage had already been done however, and the brand faded into obscurity, with operators and developers moving on to other brands/organizations.

1.3 Ivanti and Fortinet – The Infrastructure Issue continues

It has become quite difficult to keep on top of the steady stream of Ivanti ConnectSecure zero-days, vulnerabilities, patches, and patch bypasses, but yet another ConnectSecure CVE was announced in early February, CVE-2024-22024. Ivanti stated that their original mitigations would protect against exploitation, and there was no evidence of ITW compromise, but that patching remained critical. An interesting report from Orange CyberDefence (OCD) regarding exploitation of one of the earlier ICS CVEs illustrates that very well.

In February PoC code was released for CVE-2024-21893, and OCD reported that they then observed exploitation of that vulnerability less than 5 hours later. Just over 24 hours after that they detected indicators of compromise on 670 ICS appliances. It should be noted that the 24-hour delay may reflect how long it took Orange to derive and implement a detection, not how long it took the actor to compromise that many appliances.

However, as bad as the last 2 months have been for Ivanti and their customers, Fortinet, another key industry player in the sector, has also experienced CVE related issues. On February 7th, Fortinet published CVE 2024-23108 and CVE-2024-23109 as additions to an advisory they had originally published for CVE-2023-34992, a critical remote code execution vulnerability in their FortiSIEM product. However, they then stated that they had been published in error, that they were not new zero-day vulnerabilities, and they were just duplicates of the original 2023 CVE which had been created by an API error. Later that day, a researcher at Horizon3 stated that they had discovered the two new zero-days, both of which were patch bypasses for CVE-2023-34992. After this Fortinet confirmed that the researcher was correct and there were two new critical 9.8 CVSS RCE zero-days in their products.

The following day, on the 8th of February Fortinet published CVE-2024-21762, a critical 9.8 CVSS RCE zero-day in FortiOS and FortiProxy appliances, which on the 9th of February was added to CISA's Known Exploited Vulnerability (KEV) catalogue, indicating that it was known to have been exploited by attackers. All of this boils down to the issuing of three critical zero-days for Fortinet enterprise appliance products over three days.

This is part of an ongoing and serious trend described initially in January's Threat Landscape Update: Vulnerabilities in Infrastructure appliances and the struggle to patch them. It was likely difficult to keep track of these vulnerabilities internally, even when those vulnerabilities were critical zero-day RCEs, which is problematic for organizations who need to urgently patch them.

Returning to Ivanti, researchers at Eclypsium inspected the Ivanti Connect Secure Linux OS image and found a number of concerning issues. Software and OS components were identified that were up to 21 years old, and the Linux kernel for the OS was version 2.6.32, which reached end of life in February 2016. They found that the majority of the ConnectSecure GUI is written in Perl, which makes the very old Perl version that was in use more concerning. Considering the age of the software used vulnerabilities in the product may be expected as in the last 21 years software, and system design methodologies and paradigms have changed, as have the tools available to developers, and even the level of security awareness. However, this research tells us that changing and updating appliances without impacting their function can be quite a difficult task. That is concerning considering that multiple times this year already, patches haven't been made available for vulnerabilities exploited as zero days for up to weeks after disclosure, by a number of different vendors.

Unfortunately, considering the great success that attackers of all types have had performing mass exploitation of infrastructure, we will almost certainly see more vulnerabilities and campaigns in this space in the near future.

2 Ransomware: Trends and notable reports

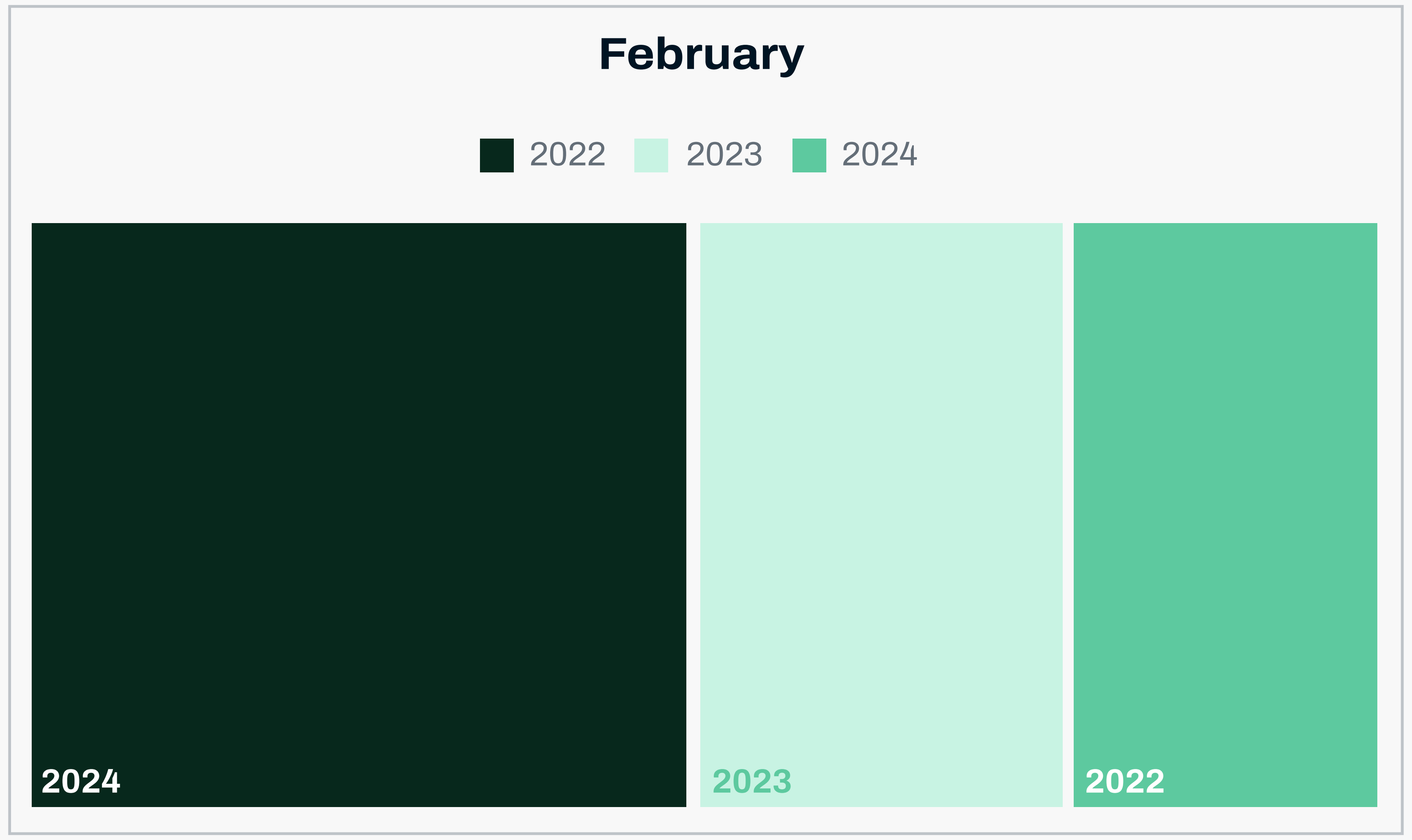
The following data is limited to ransomware and data leak groups who operate a leak site which is parseable. The following data was captured between 1st February– 29th February 2024.

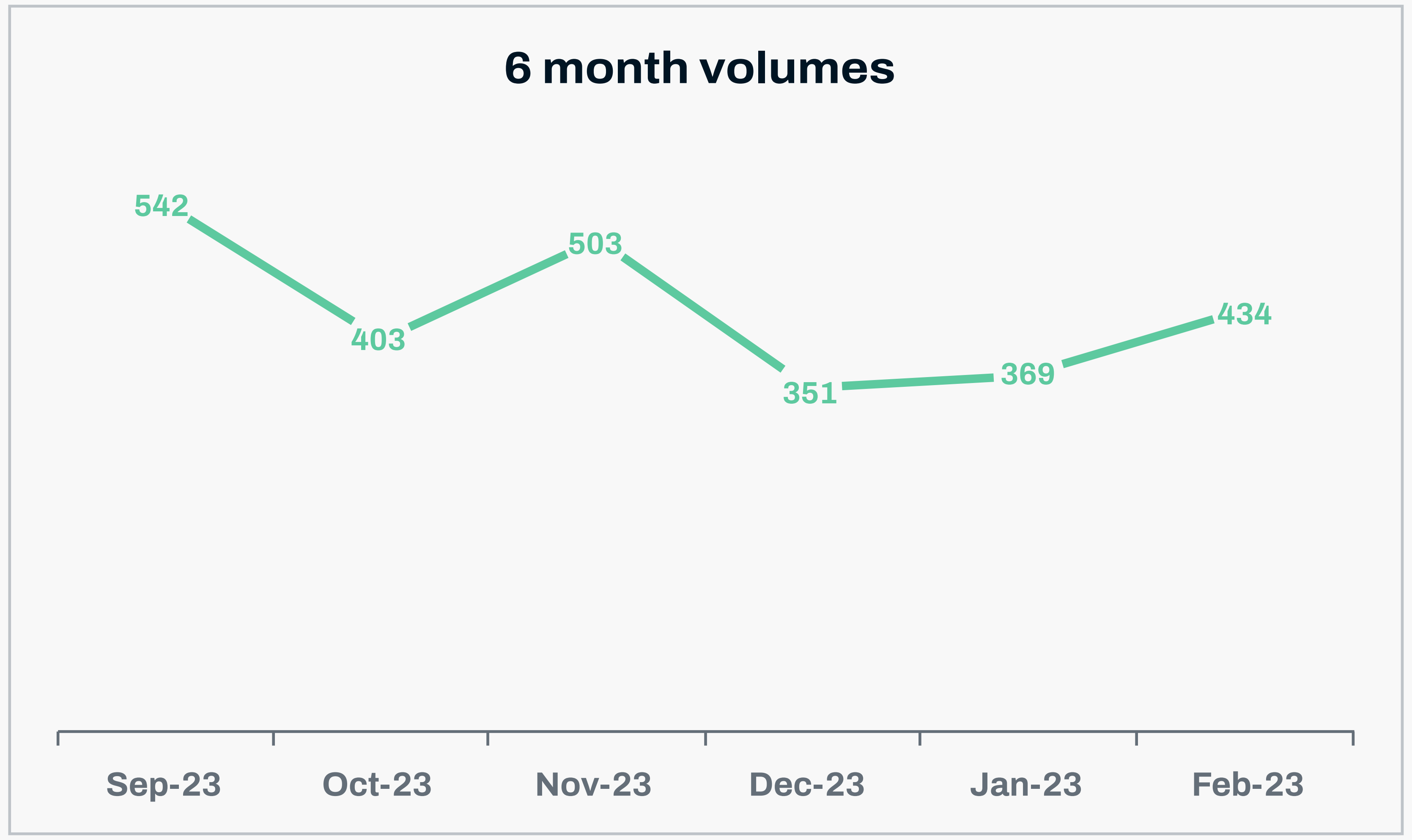
Ransomware	Jan '24	Feb '24	Change	Percentage
0mega	1	0	-1	-100
3AM	2	6	4	200
8BASE	44	23	–21	–48
Abyss	3	6	3	100
Akira	28	16	–12	–43
Alphv (BlackCat)	31	45	14	45
BianLian	17	21	4	24
BlackBasta	19	24	5	26
Blackbyte	0	6	6	-
Blackout		2	2	-
Blacksuit	4	0	–4	–100
Cactus	7	7	0	0
CiphBit	1	1	0	0
CL0P	1	0	–1	–100
Cloak	1	3	2	200
Cloak Ransomware	4	0	–4	–100
CUBA	1	1	0	0
Data Leak	1	5	4	400
Donut Leaks	0	4	4	-
DragonForce	2	5	3	150
Dunghill Leak (News)	1	2	1	100
Everest	3	1	–2	–67
Hive	0	0	0	-
Hunters Inter-tio-l	15	33	18	120
INC Ransom	10	4	-6	-60
Insane	1	0	–1	–100
Knight	11	5	–6	–55
La Piovra	0	0	0	-
LockBit	92	107	15	16
MalekTeam	1	0	–1	–100
Medusa	12	14	2	17
Meow	1	6	5	500
Mogilevich		5	5	-
Money Message	1	0	–1	–100
Monti	2	2	0	0
MyData	7	1	–6	–86
Play	4	26	22	55
Qilin	11	11	0	0
Ransomed	1	3	2	200
RansomExx	2	0	–2	–100
Ransomhouse	5	7	2	40
RansomHub	0	7	7	-
Rhysida	0	4	4	-
slug	1	0	–1	–100
S-tch	6	2	–4	–67
Stormous	2	6	4	200
Trigo-	10	4	–6	–60
Trisec	0	3	3	-
Underground	0	6	6	-
Unsafe	3	0	–3	–100

2.1 Observations

Ransomware numbers have risen for the third month in a row. Disruption of Lockbit’s infrastructure by Law Enforcement (LE) has not curtailed the numbers reaching Lockbit’s blog, however this is not a symptom of LE failure. It is reasonable to assume that organizations are better able to recover as a direct result of the action and therefore have less need to pay the ransom, therefore getting added to Lockbit's breach site in increasing numbers. In terms of long-term impact to the Lockbit brand, we will need to wait and see. The fact that February is one day longer this year is the thinnest of silver linings, as February’s numbers are over double that of February 2022, and almost double that of February 2023.

We saw five new ransomware leak sites this month: Trisec, Underground, RansomHub, Mogilevich and Blackout. Of particular note is Mogilevich which victims posted that include Shein, the Department of Foreign Affairs for Ireland, Epic Games and Nissan North America. The Irish Ministry of Foreign Affairs has stated there is no evidence to suggest they have been compromised and as the group requires a $1000 deposit to become an affiliate, there is some skepticism over whether they are legitimate operators.





2.2 Romanian Ransomware wave caused by supply chain attack

This month around 100 hospitals in Romania were affected by a wave of Phobos ransomware attacks. The volume of attacks in a short timeframe, and the close logical association of the victims (all being hospitals, and all in Romania) strongly implied that the cause was a supply chain attack. This has now been confirmed by the Romanian Cyber defense agency. The campaign began with the compromise of Romanian Soft Company's Hipocrate Information System, an integrated healthcare management system platform. Fortunately, most hospitals have backups in the past 1-3 days, however they will still lose some data, which in a healthcare environment could be critical. Targeting of healthcare institutions internationally has been on the rise in recent months, most likely due to the life-or-death consequences of operational disruption. Indeed, US cyber authorities have recently issued a warning to the healthcare sector regarding targeted ransomware attacks by the ALPHV ransomware brand.

2.3 Ransomware statistics

A number of reports containing statistics about ransomware have been released this month, often containing quite interesting, attention-grabbing statistics.

According to Cybereason, over 78% of organizations who paid a ransom demand were hit by a second ransomware attack, often by the same actor, and of that 78%, nearly two thirds of them were asked to pay a larger ransom the second time. It's an interesting and concerning set of statistics, and while compared to our telemetry 78% is possibly a high number; WithSecure certainly observe re-infection of victims. Ransomware actors cannot be trusted when claiming they will not re-infect victims and we will never encourage payment of a ransom based on trust in a ransomware operator. As such we welcome such research that gives definite metrics around the untrustworthiness of ransomware actors. Payment of ransoms is (currently) a choice that businesses have to make, but they should enter such a process with their eyes open, armed with as much information as possible.

Statistics published by Coveware state that in Q4 2023 ransomware payment rates dropped to 29%, and the average ransom payment dropped by 33% compared to Q3, to $568,705 dollars. Coveware suggest that this is due to a decline in the size of victim organizations, which they report saw a 32% drop compared to Q3 2023. Coveware state this may be linked to an increase in the number of "small game" actors who specifically target smaller organizations.

While Coveware's data covers Q4 2023 specifically, recently released statistics by Chainalysis for the whole of 2023 show that total ransom payments in 2023 doubled compared to 2022, and increased by 10-15% compared to 2021, rising to $1.1 billion.

When looking at ransomware statistics, we often use the analogy that analysis of the ecosystem is like looking through a telescope backwards, where every organization has a different view and perspective. These statistics, when combined could paint a picture of a ransomware environment where payment rates are lower, and total cost is higher – more organizations are being impacted. However, to balance this we note the time periods are different in the two research pieces and wish to reiterate the complexity of the landscape and gaps in the information we have.

3 Other notable highlights in brief

3.1 Lazarus Group disable security with Windows driver zero-day

As part of Microsoft's patch Tuesday this month, they patched a vulnerability in the AppLocker driver appid.sys, CVE-2024-21338, which could be exploited by an attacker with administrative access to disable security tools. It is the same as a BYOVD attack, but without the need to "Bring your own", instead the vulnerable driver was present on all modern Windows systems. Avast report that this vulnerability was exploited by North Korean state sponsored hackers Lazarus Group, to deploy their FudModule rootkit.

3.2 I-Soon leaks reveal details of China's state funded hacking ecosystem

I-Soon is a Chinese company which is contracted to perform hacking for hire for the Chinese government. Recently an extremely large trove of data from I-Soon was leaked online, and researchers have been mining the data for insights since then. Researchers from Pinnacle and Sentinel One have provided their analysis, noting that most of the hacking activity was a direct result of contracts from government agencies, and was directed to support the achievement of China's Five Year Plan. Researchers at Margin concluded that the businesses in this Chinese ecosystem operate much like Western hack-for-hire businesses, such as NSO group, and Hacking Team. They also note that Chinese Antivirus firm Qihoo360 invests in offensive capabilities firms, and may be selling the PII of individual antivirus customers to a Qihoo funded company that works for Chinese government intelligence clients. They also state that the leaks confirm the Tianfu Cup (similar to Pwn2Own) is likely to be a vulnerability feeder system, and that Chinese hacking firms use partnerships with ministries of education and defense contractors to run capture-the-flag competitions to attract talent.

3.3 Anydesk source code and signing keys stolen

This month RMM provider AnyDesk stated that hackers gained access to production systems, stealing source code and private code signing keys. AnyDesk have stated that no customer data was stolen, no unauthorized access to customer environments was detected, and while they did reset all passwords to access their online portal, they stated that this was done out of an abundance of caution, not in response to any detected activity. The stolen code signing certificate has been revoked, and a new version of AnyDesk released which has been signed with new certificates.

Amusingly, at one point it appeared that this might be one of the major stories of the month.

3.4 AWS SMS service abused on compromised clouds for bulk smishing

Researchers at SentinelOne reported on a malicious python script named SNS Sender that can use the AWS Simple Notification System (SNS) to bulk send SMS messages and is being advertised to threat actors as a bulk Smishing tool to monetize compromised AWS environments, an interesting and innovative pivot that could lead to even more missed package notifications for everybody.

3.5 Researchers weaponize LLMs to independently hack vulnerable sites

Researchers at a US University have been able to train LLM powered agents equipped with tools for accessing APIs, automated web browsing, and feedback-based planning, to autonomously hack vulnerable websites without operator oversight. The agents have been observed to perform attack processes up to 38 steps long culminating in actions such as a SQL Union attack. It is important to note that the agents only operated within a sandboxed environment, the researchers did not perform these activities on the Internet, although there is nothing to prevent less scrupulous actors from doing so.

3.6 iOS banking trojan campaign leverages AI fakes for fraud

The Bank of Thailand recently instructed banks operating in the country that bank transfers over a certain size will require facial biometric verification. Researchers at GroupIB have published analysis of an iOS trojan they name GoldPickaxe which is targeting victims in Thailand. As well as abusing Mobile Device Management and social engineering to gain access to victim devices, GoldPickaxe prompts victims to record video of themselves which the attackers can then use to generate AI-face swapped video to approve large bank transfers, bypassing the Thai requirement for facial recognition approval.

3.7 US Credit Union software vulnerabilities – One for all and all for one – In a bad way

Researchers at LMG security identified vulnerabilities in CUSG CMS, a CMS software used by hundreds of Credit Unions in the US. These include the ability to intercept login credentials from the admin portal, and the ability for any authenticated user to gain full read/write access to the backend database, which in every single customer installation contains the static password to an “ultra admin” account which exists in every customer installation, and has full administrative access. Using this an attacker could have compromised any vulnerable customer, obtained the ultra admin password, and then accessed any other customer environment that did not require MFA. Fortunately, the developer of this software issued a patch prior to the vulnerability announcement, though that does not necessarily mean that all users of the software applied that patch.

3.8 Qakbot, Bumblebee and Pikabot evolve

New variants of three commodity malware families have been observed, in the case of Qakbot and Bumblebee after a short hiatus. In each piece of malware there is evidence of recent changes to the codebase and software versions. In the case of Qakbot, formerly a titan of this landscape up until the infrastructure takedown in late 2023, the volume of activity observed is very small indeed, and in no way indicates a return to power just yet. Bumblebee has returned from a 4-month hiatus with a seemingly low effort voicemail phishing campaign to deliver an office document VBA macro to drop a wscript file. Pikabot has debuted a new version that researchers describe as “devolved”, where the complexity of the code has been reduced, certain obfuscation techniques removed, and the C2 network comms changed.

3.9 Attackers compromise crypto gaming platform – take lots of money

PlayDapp is a cryptocurrency-based gaming platform, and as often seems to happen with cryptocurrency platforms recently, it has been hacked and had a large amount of money stolen. Initially, attackers were able to create 200 million tokens worth $36 million dollars based on market value at the time, with reporting suggesting this was possible due to a stolen private key. PlayDapp then messaged the attacker offering a $1million dollar reward and no law enforcement involvement if they returned the stolen money. Several days later, the attackers responded by creating another 1.59 billion tokens. The exact value of those 1.59 billion tokens is unclear, as it is based on market value, and at a very basic level the more tokens there are, the less valuable they are. In addition, a cryptocurrency which has recently been comprehensively hacked and devalued is unlikely to be trusted or valued, which could lead to an even greater drop in value.

3.10 Deepfake scam uses AI faked conference call

This month it was reported that the Hong Kong office of a multinational corporation was the victim of an AI deepfake scam, losing over $25 million. The attackers sent a phishing message to a user in the Hong Kong branch which purported to be from the UK based CFO of the organization. While the recipient was suspicious, they were then invited onto a group video call with the CFO and multiple other employees where they were instructed to make 15 transfers in total. It was not until a week later that the theft came to light, and it was realized that all the participants on the call had been faked using AI technology.

3.11 Russia arrests ransomware group members for some reason

Newsworthy if only for its novelty, Russian law enforcement agencies recently arrested three alleged members of the SugarLocker ransomware group. SugarLocker is believed to be associated with the REvil ransomware group, and the arrested individuals were operating under the guise of a legitimate tech company named Shtazi-IT. It is unclear why Russian LEAs would take action against cyber criminals, when they so famously do not, or why they acted against these alleged criminals in particular.

3.12 MS Expands logging capability

After a number of serious compromises of Microsoft customers, and, as mentioned last month, of Microsoft themselves, the software company have announced that they are upgrading the free level of logging capabilities for all Purview Audit Standard customers. It is worth noting that this includes US Federal agencies, and that between May and June of 2023 Chinese state hackers had access to US government emails in Exchange Online, something that may well have been undetectable without additional, more detailed logging that Microsoft at the time charged extra for. This complimentary upgrade of logging capabilities was stated to be arranged with the input of CISA, the US Office of Management and Budget, and the Office of the National Cyber Director.

3.13 SSH Snake post exploitation worm

A new, open-source, post exploitation tool named SSH-Snake has been identified by Sysdig. SSH-Snake is a self-modifying, self-propagating worm written in bash which will search for SSH private keys in various locations, then attempt to use them to spread to other systems it identifies on the network, where it will attempt to do the same. Details of the accesses and systems the worm identifies are returned to the attacker.

4 Threat data highlights

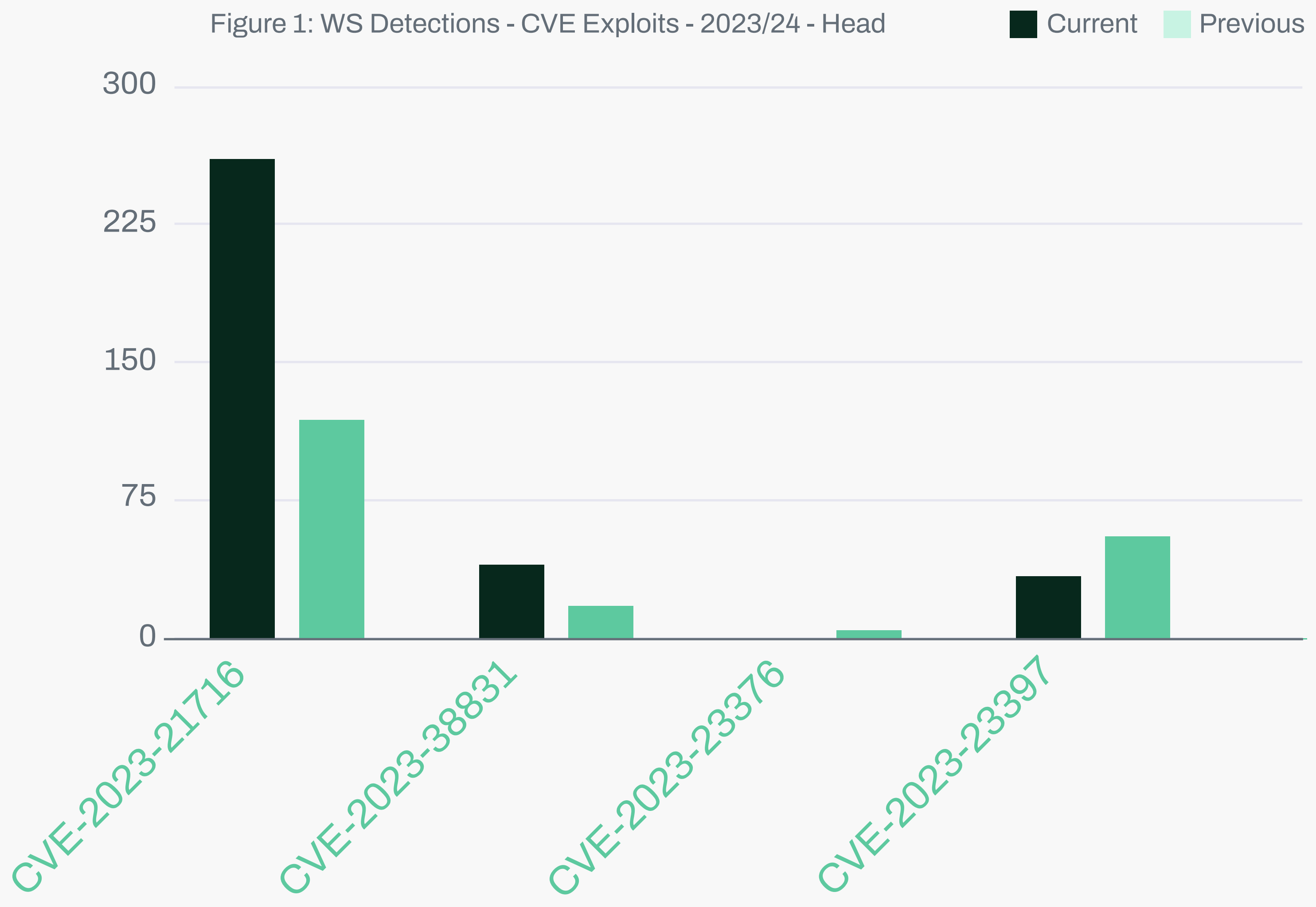
4.1 Summary

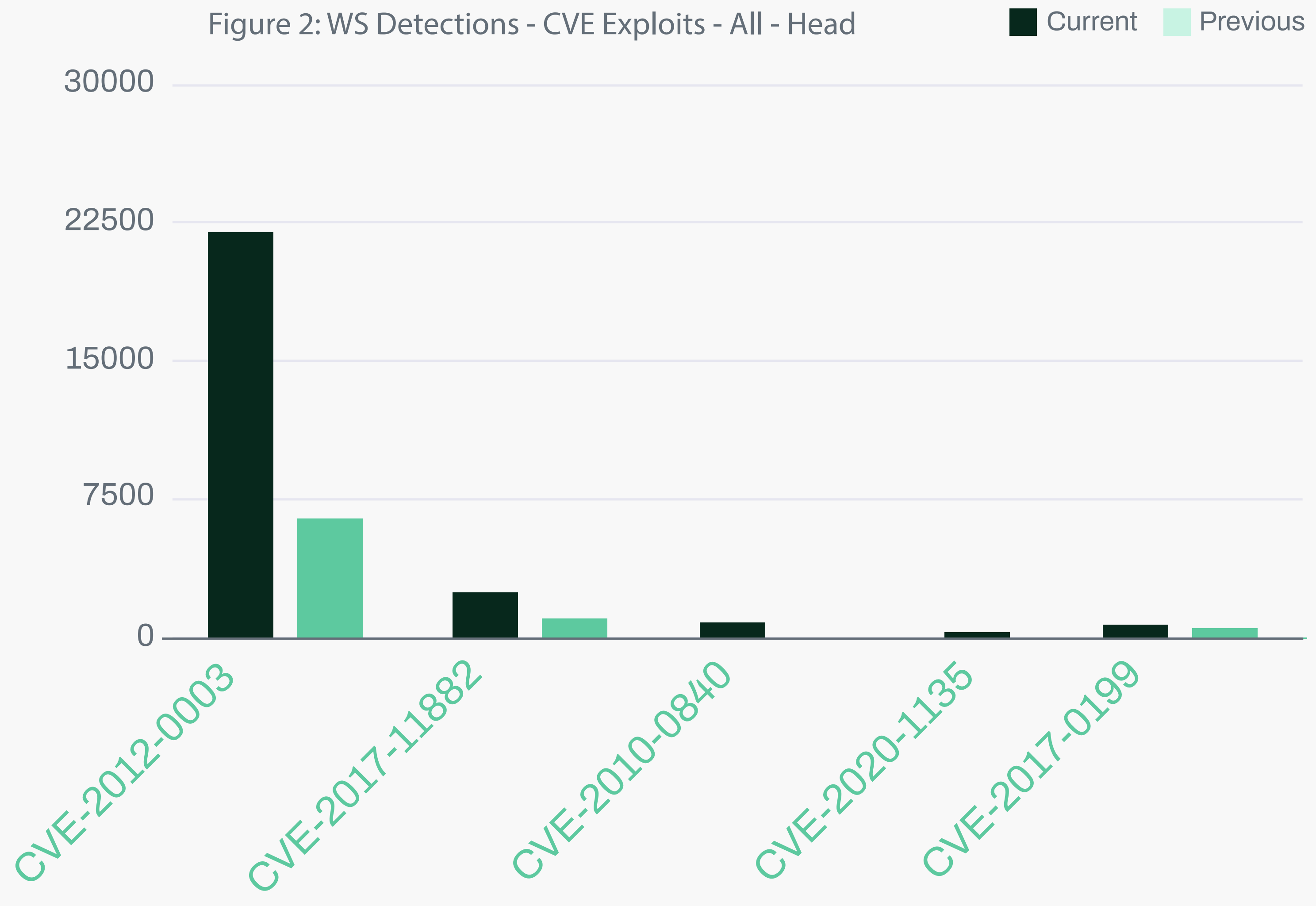
There were significant increases in a number of typical phishing/maldoc exploits targeting client software in the previous 30 days. While the news over the previous two months has been heavily concerned with server and infrastructure vulnerabilities, it is of course expected that detection data will be dominated by client targeted phishing and maldoc exploits like this, as firstly there are far more client devices than servers/infrastructure, and a far higher percentage of them will be running EDR/EPP. Secondly, every stage of compromise is less likely to occur than the stage before. Maldocs get delivered via phishing, the vast majority are detected and prevented from successfully executing/exploiting, and so the number of incidents that progress beyond this point will be much lower.

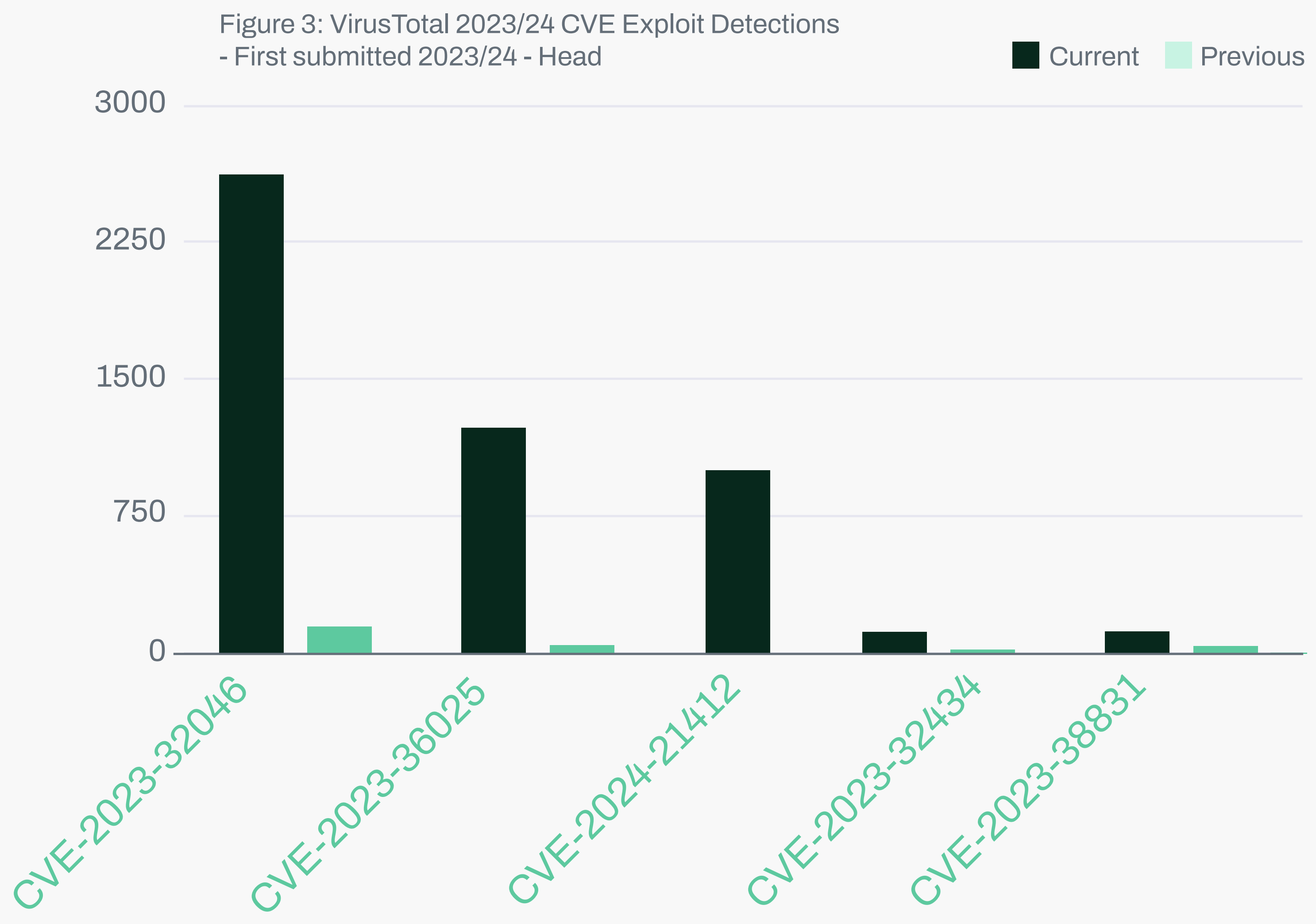
4.2 Exploit data

WithSecure detection data for 2023/24 CVE exploits this month (Figure 1) shows a significant rise in CVE-2023-21716, which is a Microsoft Office/Word/SharePoint RCE triggered by viewing a crafted RTF file. The exploit detections for this vulnerability have doubled for the second month running. The WinRAR vulnerability CVE-2023-38831 has also increased in volume, detections of this exploit have been variable but ongoing since it first came out in late 2023. Of note is that detections of this exploit in the VirusTotal data have also risen significantly, mirroring our internal data.

Finally, CVE-2023-23376, a Windows Common Log File System privilege escalation vuln, and CVE-2023-23397, the recent Outlook custom notification NTLM hash harvesting vuln, have both dropped in volume this month. Interestingly, CVE-2023-23397 rose in VirusTotal's stats, however we speculate that this vulnerability is so low effort/high effect that it is likely that it will continue to be used by threat actors for some time and will likely become part of the background noise of exploit data in future, ever present but not necessarily significant.







Looking at WithSecure exploit data for older vulnerabilities there was a significant increase in a number of vulnerabilities, with the largest increases in CVE-2012-0003 (Windows RCE via crafted Midi file) and CVE-2017-11882 (MS Office equation editor RCE). CVE-2012-0003 has been on a dramatic upwards trajectory for two months now, increasing from 60 to 6,000 last month, then increasing 400% this month. The increase in exploitation of CVE-2017-11882 was also seen in VirusTotal data. There were smaller real terms increases in CVE-2010-0840 (JRE) and CVE-2020-1135 (Office Wordpad RCE), but as percentage increases, they were far larger, with exploits of the CVE-2020-1135 increasing 10,000% (100 times over) compared to last month, and CVE-2010-0840 vulnerability increasing 1,000%

Moving on to look at VirusTotal exploit data (Figure 3) there have been huge rises in detections of CVE-2023-32046 (MSHTML Privesc), CVE-2023-36025 (Windows SmartScreen bypass via .url files), and CVE-2024-21412 (Water Hydra's bypass for CVE-2023-36025). There was also a large increase in CVE-2023-32434 (MacOS Privesc). Considering the relative install base size of Windows and Mac, the appearance of a Mac vulnerability in this top 5 detections means that within the Mac ecosystem this exploit must be extremely common.

Of note, while it didn't make it into the top 5 there was also a spike in files exploiting CVE-2023-46805, which is an Ivanti ConnectSecure Auth bypass, one of the first two ICS zero-days from January.

4.3 Newly Exploited Vulnerabilities

The following vulnerabilities have been added to CISA's Known Exploited Vulnerabilities catalogue in January:

CVE ID	Vendor	Product	Name	Description
CVE-2023-4762	Google	Chromium V8	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8 contains a type confusion vulnerability that allows a remote attacker to execute code via a crafted HTML page. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.
CVE-2024-21762	Fortinet	FortiOS	Fortinet FortiOS Out-of-Bound Write Vulnerability	Fortinet FortiOS contains an out-of-bound write vulnerability that allows a remote unauthenticated attacker to execute code or commands via specially crafted HTTP requests.
CVE-2023-43770	Roundcube	Webmail	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail contains a persistent cross-site scripting (XSS) vulnerability that can lead to information disclosure via malicious link references in plain/text messages.
CVE-2024-21412	Microsoft	Windows	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Windows Internet Shortcut Files contains an unspecified vulnerability that allows for a security feature bypass.
CVE-2024-21351	Microsoft	Windows	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows SmartScreen contains a security feature bypass vulnerability that allows an attacker to bypass the SmartScreen user experience and inject code to potentially gain code execution, which could lead to some data exposure, lack of system availability, or both.
CVE-2020-3259	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Cisco ASA and FTD Information Disclosure Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) contain an information disclosure vulnerability. An attacker could retrieve memory contents on an affected device, which could lead to the disclosure of confidential information due to a buffer tracking issue when the software parses invalid URLs that are requested from the web services interface. This vulnerability affects only specific AnyConnect and WebVPN configurations.
CVE-2024-21410	Microsoft	Exchange Server	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server contains an unspecified vulnerability that allows for privilege escalation.
CVE-2024-1709	ConnectWise	ScreenConnect	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect contains an authentication bypass vulnerability that allows an attacker with network access to the management interface to create a new, administrator-level account on affected devices.

5 Research highlights

5.1 Windows KrustyLoader caught and identified by WithSecure

On the 21st of February proof of concept code for CVE-2024-1708, a ConnectWise ScreenConnect zero-day authentication bypass was published. On the 22nd of February WithSecure observed exploitation of the ScreenConnect vulnerability being used to deploy a previously unknown Windows variant of a loader malware dubbed KrustyLoader. KrustyLoader was first named by Synacktiv in January 2024 when analyzing implants dropped during mass exploitation of Ivanti ConnectSecure devices. While investigating the activity we were also able to link it to previously documented campaigns from late 2023 which exploited critical vulnerabilities in JetBrains TeamCity and ApacheMQ. As such we assess that the intrusion set behind this activity has been continually targeting edge vulnerabilities for some time, possibly acting as an Initial Access Broker, though we do not have insight into actions on objectives after a Sliver post-exploitation framework is deployed, an attack step common across all noted campaigns.

This research was published in full on the WithSecure Labs blog on the 24th of February.

5.2 Binary exploitation for SPECIAL occasions, and The hidden depths of mainframe application testing

A pair of articles by Alex Gassam and Leandro Benade, respectively. Alex's article on privilege escalation in z/OS is an introduction to low level memory and binary exploit development for those interested in mainframe security. Leandro's article highlights the broad attack surface of mainframe applications, and while it focuses on z/OS environments with RACF implemented, it covers topics and themes that can be applied to any mainframe platform. Considering the ongoing reliance on mainframes by CNI organizations, and the often-assumed security by obscurity in that realm, this is definitely a topic that is worth shining a light on.

5.3 Runc working directory breakout (CVE-2024-21626)

A research piece by Mohit Gupta gives an overview of this vulnerability in runc, and its impact on orchestration-based environments such as Kubernetes. In a Kubernetes environment an attacker with the ability to deploy pods could leverage the runc vulnerability to perform a breakout attack onto the underlying Kubernetes nodes, which could then allow the attacker to access pods from another tenant. This then could enable severe, wide-reaching supply chain attacks in cloud hosting platforms.

5.4 Should you allow ChatGPT to control your browser?

Donato Capitella presents the security risks of granting an LLM control over your browser in his research piece on the WithSecure website. The research demonstrates two exploitation scenarios using Taxy AI, a representative proof-of-concept browser agent, and also presents mitigation strategies that the developers of LLM based browser agents would need to implement to effectively safeguard users.

5.5 Multiple vulnerabilities in eLinkSmart padlocks

Alex Pettifer and Miłosz Gaczkowski present a deep dive into the security implications of eLinkSmart Bluetooth enabled padlocks which they first presented at Bsides London 2023. They chose eLinkSmart locks as the brand is popular in the UK and Germany, and has graced the front page of Amazon and the top of the Amazon best seller lists for Bluetooth padlocks. Through their research Alex and Miłosz identified vulnerabilities between the locks' implementation of Bluetooth Low Energy communication and eLinkSmart's back-end API. These vulnerabilities not only allow any lock within range to be unlocked, but also allow an attacker to retrieve the unlock times and locations of any eLinkSmart lock, even if location tracking was not enabled by the user. As so often turns out to be the case, unsalted MD5 password hashes were stored in a SQL database vulnerable to SQL injection.

Unfortunately, at no point did the Chinese vendor, eLinkSmart, respond to any vulnerability disclosures from WithSecure.

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

W/TH secure