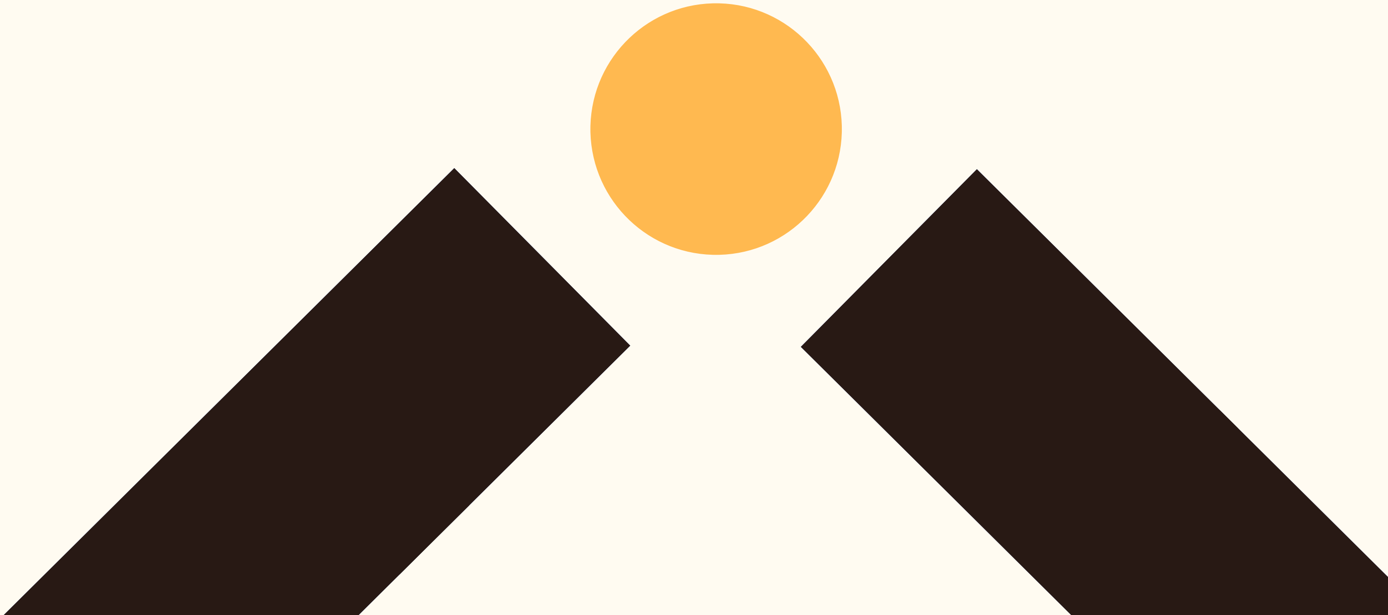
Threat Highlight Report

March 2025

Table of Contents



Foreword

"This month has seen mass exploitation of edge network devices for state espionage, but also for intellectual property theft targeting dozens of mid-sized European manufacturing companies. A compromise has also been claimed of the Oracle Cloud hosting service, which if confirmed as true could have resulted in the theft of data and credentials belonging to 140,000 client organizations.

In Ransomware it has been another record month, with more victims posted to data leak sites than in any month since we began our records. This was in large part due to Cl0p, who posted over 200 victims this month from their 2024 exploitation of a zero-day in the Cleo managed file transfer software.

Two separate campaigns have been reported this month where actors have used OAuth apps, something intended to provide security, as a way of compromising their victims, though the methods used differed slightly in each case.

This is also the time of year for annual summaries to be published, and multiple security researchers have used their data for the last year to provide statistics and summary documents from which we can draw insights as to the state of the cyber threat, and of cyber defenses.

This month we have also released two Cyber Threats Xposed podcasts, one on our normal schedule, and another specifically discussing the threats to the European mid-market. Do check them out via your usual podcast channels."

Stephen Robinson,
Senior Threat Intelligence Analyst, Threat Intelligence and Outreach, WithSecure

Monthly highlights

The international problem of mass exploitation

This month saw further reporting on the international mass exploitation of Ivanti network edge devices by Chinese actor UNC5337. The Ivanti Connect Secure vulnerability CVE-2025-0282 has been targeted by the actor to deploy variants of their rapidly evolving SPAWN malware family. This activity has been reported by the Japanese national CERT, Mandiant, and now CISA. In each case different versions of the SPAWN malware were observed being deployed directly onto the compromised Ivanti devices. The latest notification is from CISA and details a malware called RESURGE, which along with containing a variant of SPAWN, named SPAWNCHIMERA, it also has rootkit, dropper, backdoor, boot kit, proxy, and tunneller functionality.

While we have spoken time and again of the threat of mass exploitation of edge devices, it is clear that it remains a problem. Not only does it remain a problem, it remains a difficult to solve problem, as shown by the disclosure from the Finnish Ministry of Foreign Affairs that their remote access service was compromised this month. What is most interesting about the information released so far, is that they knew that their remote access service was vulnerable back in 2024, however they could not patch or mitigate the vulnerability, and they could not operate without the remote access service. As such, the only thing they could do was keep using the service while putting in place enhanced security monitoring. It appears that this enhanced monitoring rapidly detected the compromise, leading to the service being taken offline, however at present it is unclear just what impact there may have been.

WithSecure Insight

The warnings from CISA, JPCERT, and Mandiant should be concerning to any organization that is running any enterprise grade network edge security devices. The SPAWN malware is yet another example of network infrastructure resident malware, as was seen when threat actors deployed sliver to compromised PanOS devices during one of the Palo Alto/PanOS exploitation campaigns in late 2024. A big problem with infrastructure resident threats is that it exists where XDR tools cannot, unless the user is willing to breach the terms of their license and support agreements with their network infrastructure suppliers.

The situation the Finnish Ministry of Foreign Affairs found themselves in, where they knew their remote access service was vulnerable, but they had no choice but to keep using, it is probably a situation that many organizations have experienced in recent years. In such a situation there really is no option except to greatly enhance security monitoring and apply defense in depth measures, but of course not all organizations will have the resources or capability to do even that.

Claim of Oracle Cloud breach, possible theft of 6 million records belonging to 140,000 tenants

An attacker is claiming to have breached Oracle Cloud, stealing customer security keys and sensitive data. While Oracle has denied that Oracle Cloud has been breached, an artifact left on an Oracle server by the attacker, as well as sample data provided by the attacker and verified by security researchers and Oracle Cloud customers strongly suggests that there has been a breach. The probable breach involved exploiting a vulnerability in Oracle Fusion Middleware's Oracle Access Manager, which can give intruders access to sensitive information.

While this breach has so far been denied by Oracle, they have notified customers of their Oracle Health service (known as Cerner before it was bought out by Oracle) that they are aware of a breach of the PII of patients of US hospitals which came to light in February. Slightly ironically, it appears that this breach only affected data that was still stored on former Cerner physical servers. Oracle's notification states that any Oracle Health data that was moved to Oracle Cloud was not known to be affected by that specific breach.

WithSecure Insight

A breach of the Oracle Cloud login servers, as has been claimed, could be a devastating supply chain attack. The situation of Oracle's customers (and their customers) is complicated by the fact that Oracle are denying the breach, while sample data from the threat actor has apparently been verified by multiple Oracle customers and security researchers. While cloud services try to appear simple, they are in fact extremely complex, and so it may be possible that users of Oracle Cloud could be compromised without it technically being due to a breach of Oracle services, however at present there is no information to indicate that is the case, and for the customers and downstream customers who might be affected that distinction would be of little comfort.

Checkpoint firewalls exploited in targeted industrial espionage against mid-market European and EMEA manufacturers

A Chinese APT group, likely APT41, exploited a path traversal vulnerability (CVE-2024-24919) in Check Point security gateways to infiltrate dozens of OT organizations globally. The attackers used specially crafted requests to access sensitive files, including password hashes, enabling them to gain superuser privileges and install the ShadowPad backdoor for espionage purposes. The campaign, which began shortly after the vulnerability was disclosed in May 2024, peaked in November and continued until last month. Researchers have not observed any disruption caused by the attackers, who focused on stealing valuable intellectual property.

WithSecure Insight

This campaign shows that exploitation of edge devices for the purposes of stealthy data theft is not just an issue for government agencies. Most organizations will hopefully be aware that vulnerable Internet facing devices can lead to destructive attacks such as ransomware, but over stretched Security and IT teams may not be on the lookout for stealthy data theft. The threat of international IP theft has been known for many years now, and it may even become more common as international trade is disrupted by tariffs and geopolitical friction.

Ransomware

The following data is limited to multi-point of extortion groups who are operating a leak site which is parseable. In this section we will be looking at victim leak sites. This dataset is probably the best and most consistent source we have that enables us to understand the landscape, but the data collected here is not fallible, there are several variables that impact and skew this dataset:

- It is attacker led, and some attackers may be incentivized to post incorrect data.
- It is fluid, and victims are added and removed frequently.
- Extortion success is another key factor, if the amount of paying victims greatly increases, 'total' ransomware numbers may also appear to decrease.

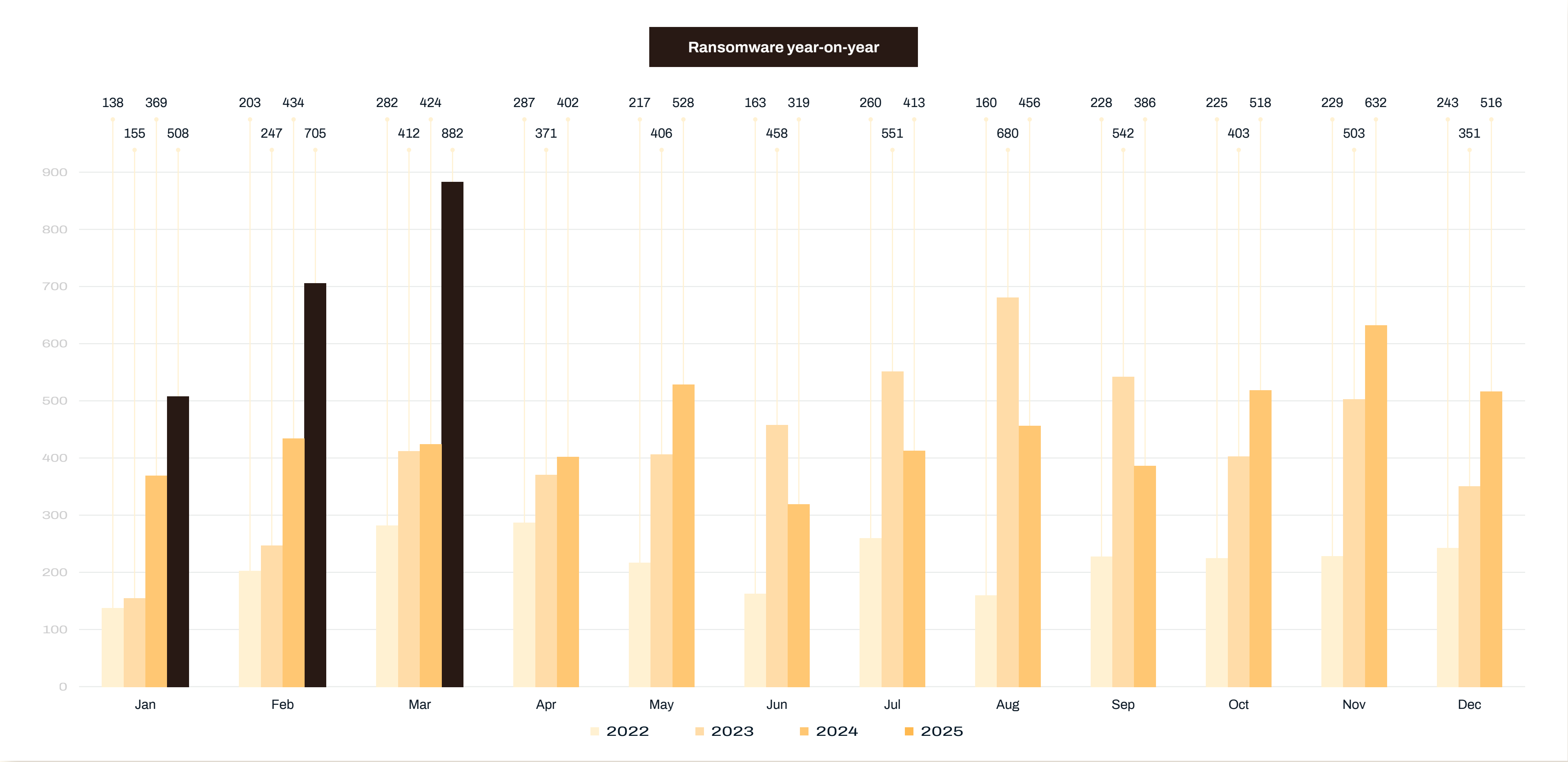
With this said, we can draw some insight from this data with sensible assumptions – and recognizing the data isn't perfect, it does provide a decent gauge on the ransomware landscape.

The assumptions the industry typically abide by are:

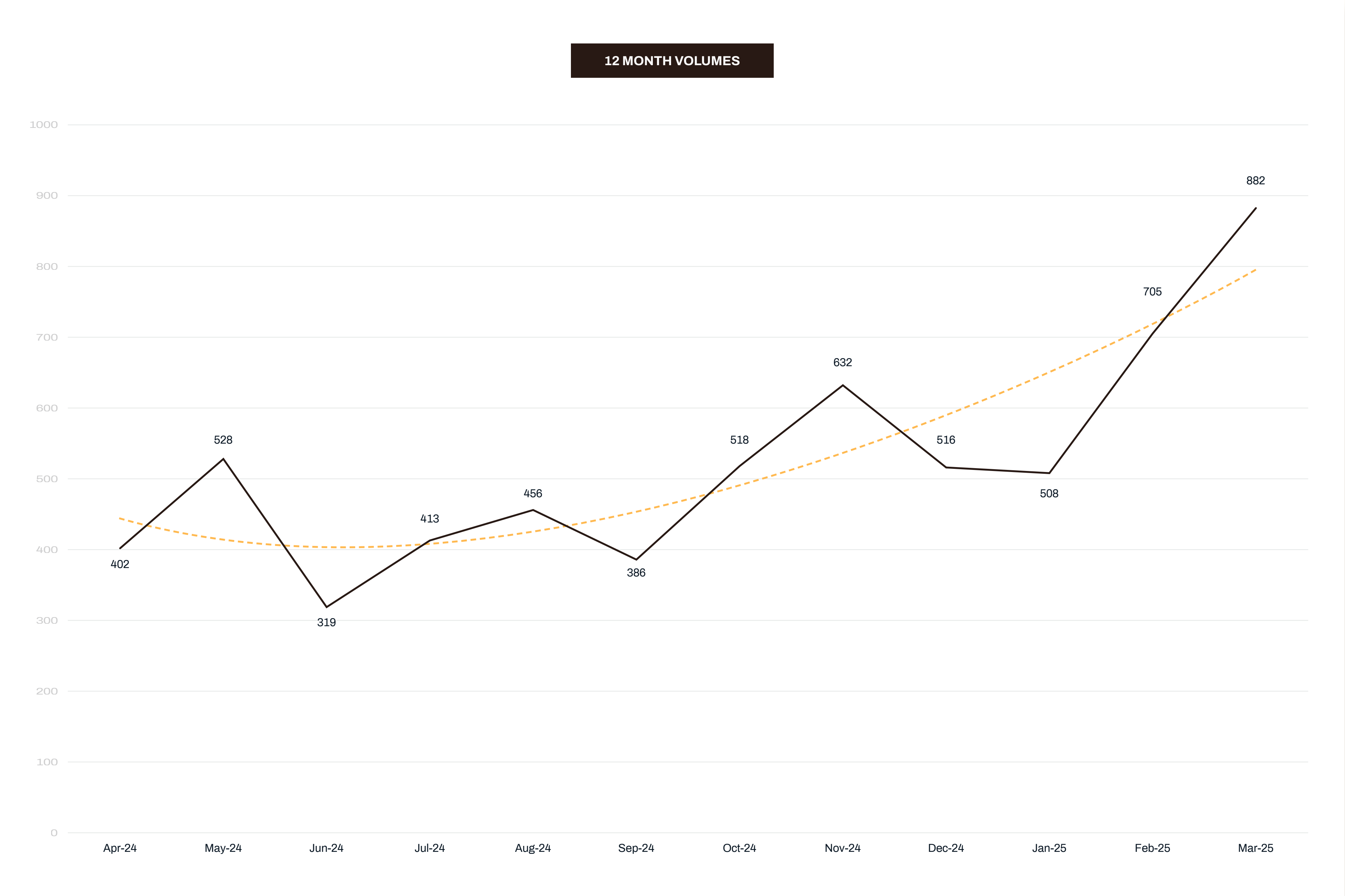
- There is a roughly relatively consistent month-on-month victim payment rate,
- Actor posts do contain an element of truth.

March ransomware statistics

March has surpassed February's recording breaking month (705) with 882 victims. This does not include 94 BABUK2.0 victims, which have been excluded from the total count as the validity of many of their victim postings was doubtful. CL0P have continued posting victims from the Cleo's MFT mass compromise. Their total victim count increased by 124 to 217. Increases in victims from Safepay, INC Ransom, and Akira have also contributed to a rise in numbers, alongside newcomers Frag, Nightspire and CrazyHunter. These increases weren't much offset by reductions in numbers posted from Cactus (-28), Play (-17) and RansomHub (-15).



Ransomware year-on-year


12 MONTH VOLUMES
1000
900
800
700
600
500
400
300
200
100
0
402
528
319
413
456
386
518
632
516
508
705
882
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
Nov-24
Dec-24
Jan-25
Feb-25
Mar-25

March ransomware victim volumes

Top 20 March			
Leak Site	**Feb**	**March**	**Delta**
CL0P	93	217	124
BABUK 2.0*	**-**	**94**	**94**
RansomHub	103	88	-15
Akira	58	68	10
Qilin	42	47	5
Safepay	13	42	29
Fog	43	32	-11
Play	48	31	-17
Lynx	33	30	-3
INC Ransom	13	30	17
Frag	0	27	27
LeakedData	9	23	14
Kill Security	22	20	-2
Medusa	34	18	-16
NightSpire	**-**	**16**	**16**
DragonForce	7	15	8
Arcus Media	5	15	10
BianLian	20	12	-8
Sarcoma	7	10	3
CrazyHunter	**-**	**10**	**10**

Biggest Risers

Leak Site	Feb	March	Delta
CL0P	93	217	124
BABUK 2.0	-	94	**94**
Safepay	13	42	29
Frag	-	27	27
INC Ransom	13	30	17
NightSpire	-	16	16
LeakedData	9	23	14
Akira	58	68	10
Arcus Media	5	15	10
CrazyHunter	-	10	10

Biggest Fallers

Leak Site	Feb	March	Delta
Cactus	36	8	-28
Play	48	31	**-17**
Medusa	34	18	-16
RansomHub	103	88	-15
Fog	43	32	-11
Cicada3301	13	2	-11
BianLian	20	12	-8
Eraleignews	7	-	-7
Termite	7	1	-6
Hunters International	10	6	-4

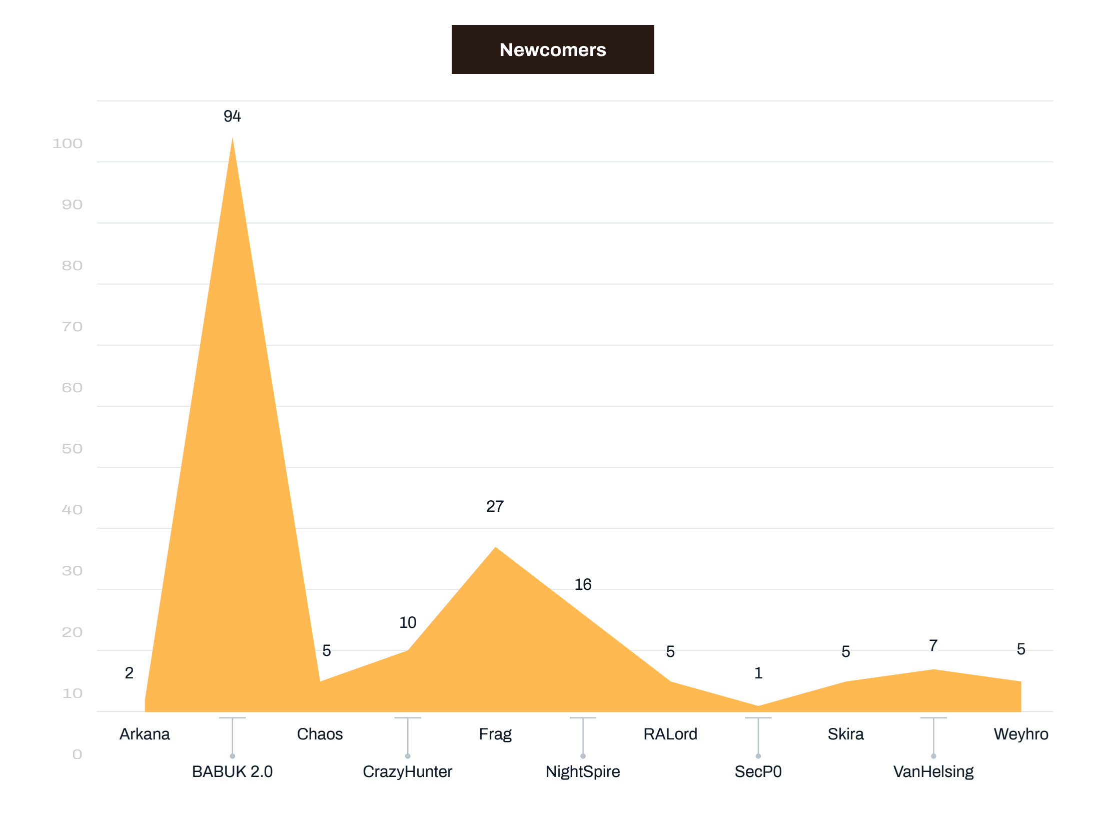
New ransomware groups

There were 11 new ransomware data leak sites (DLS) observed this month. Babuk2.0 is counted in this number, however WithSecure are not yet convinced in the legitimacy of any of its victims. The remaining 10 DLS' contributed 83 new victims.

Frag ransomware, an Akira variant, was first observed in October 2024. It is not yet clear whether this is relevant to the new 'Frag' DLS which posted a significant 27 victims in March.

CrazyHunter ransomware appears to almost exclusively target Taiwan, based off open-source ransomware code [read about that here].

Nightspire posted 16 victims, which is unusually geographically dispersed, with only 2 of the 16 victims targeting the US. There appears to be a larger-than-usual Asian victimology.



European targeting

11.42% of victiWms were based in the EU this month. The following represents the ransomware brands that disproportionately impact victims in the EU.

DLS	%EU
SAFEPAY	30.61
INC Ransom	30
Akira	26.76
Arcus Media	26.67
Lynx	25.81

Cl0p release multiple tranches of Cleo compromise victims

This month Clop added two tranches of victims to their data leak site, seemingly as a result of their Cleo managed file transfer compromise campaign. It appears that Cl0p had so many victims that they had to manage them quite methodically, as the victims split by alphabetical order.

WithSecure Insight

Cl0p have demonstrated several times that they have the capability to identify, productionize, and exploit zero-day vulnerabilities. They have also had great success in targeting managed file transfer, first with MOVEit, then Cleo. While the Cleo campaign may feel like old history by now, the sudden appearance of a large number of victims on the Cl0p leak site makes clear that behind the scenes, activity and the impact due to the exploitation campaign has been on going.

DPRK actor Moonstone Sleet acting as Qilin affiliate

Microsoft has identified that North Korean threat actor Moonstone Sleet is now deploying Qilin ransomware in limited attacks. Moonstone Sleet, formerly known as Storm-1789, has performed many different types of cyber-attacks, and was previously known to deploy their own custom ransomware variant.

WithSecure Insight

It is not unknown for state sponsored APTs to deploy ransomware, it is believed that many different groups have deployed ransomware as a form of wiper to hide espionage activity for example. However, DPRK actors are known to be motivated by both financial gain and espionage, and they have been known to deploy their own ransomware lockers. It is unusual to find a nation state acting as a ransomware affiliate in this way, however. Since Moonstone Sleet obviously have the capability to develop their own ransomware and malware this may seem a strange choice, however by using ransomware developed and maintained by another group they can increase their efficiency. They can also to some extent hide their own activities amongst that of other Qilin ransomware affiliates, making it more difficult for security services in other countries to track and disrupt their activity.

New Lockbit linked ransomware group Mora_001 exploiting vulnerable Fortinet devices

A new ransomware operator named Mora_001 is exploiting two Fortinet vulnerabilities to gain unauthorized access to firewall appliances. The actor then moves laterally and deploys a custom ransomware strain dubbed SuperBlack. The campaign has multiple links to Lockbit, including a tox messenger address, and extensive IP addresses. Multiple tool overlaps have also been observed with BrainCipher, EstateRansomware, and SenSayQ, all of which have also been associated with Lockbit.

WithSecure Insight

This could well have been listed under mass exploitation, but what is more interesting here is the links to Lockbit. Lockbit were a, if not the major RaaS operation for years, and while the brand is now essentially defunct there are multiple other groups operating now which have links to previous Lockbit activity. Such groups could have been linked to the core Lockbit organizers, or they could simply have been affiliates who worked extensively with Lockbit. The key thing is that law enforcement disruption of the Lockbit core group probably contributed to retarding the growth of the RaaS industry in 2024, possibly by breaking down the actor's trust of each other and their presumption of untouchability, but these operators and actors do still exist, and they still have the same expertise and financial motivation. Unfortunately, combatting ransomware and cyber-crime has been, is, and will be an ongoing effort.

Identity

FBI court filings link $150 million Crypto theft to the 2022 LastPass hack

U.S. federal agents have linked a $150 million cryptocurrency heist to the 2022 LastPass hacks, where thieves cracked master passwords stolen from the password manager service. The stolen data and passwords were used to access victims' electronic accounts and steal information, cryptocurrency, and other data.

The investigation revealed that the attackers targeted individuals who had stored their cryptocurrency seed phrases in the "Secure Notes" area of their LastPass accounts prior to the breaches.

WithSecure Insight

In the year after the LastPass hack there were reports stating that it appeared attackers were cracking the master passwords for the stolen LastPass data and using them in attacks targeted at high value crypto investors.

This statement by the US FBI and Secret Service reinforces those conclusions and highlights the threat of compromised password vaults. The security of password protected data is of course only as strong as the password used, and after the LastPass hack attackers had access to the data in offline environments where they could apply as much computer power as they had to brute forcing passwords.

Because cryptocurrency wallets are also protected by passwords and credentials, those credentials are a key focus of modern infostealers. As we have stated before, digital currencies which can be controlled entirely through usernames and passwords, and which are designed to bypass the modern financial system and it's many controls are the perfect target for attackers.

12,000 GitHub accounts targeted with malicious OAuth app.

An extensive phishing campaign targeted nearly 12,000 GitHub repositories with fake “Security Alert” emails, attempting to trick developers into authorizing a malicious OAuth app. The app granted attackers full control over accounts and code, allowing them to exfiltrate data to a server hosted on Render. Developers who have been targeted by this campaign are advised to revoke suspicious app access and reset credentials to prevent further attacks.

WithSecure Insight

OAuth is intended to provide a solution to securing access to cloud resources and authenticating users, however it has also been used by attackers to deliver malwareless identity attacks. Once an OAuth app is authorized the permissions granted can be used by the app developer to act as the app user, so overly permissive granting of permissions to unknown apps can present a serious security risk, and in this case would allow software supply chain attacks through the compromised GitHub accounts.

Malicious OAuth apps delivered in highly targeted phishing campaign against US and EU businesses

Cybercriminals are leveraging malicious Microsoft OAuth applications masquerading as legitimate Adobe and DocuSign apps to infiltrate Microsoft 365 accounts. The attacks are highly targeted and delivered via phishing emails from compromised email accounts. The malicious OAuth apps request minimal permissions to avoid suspicion, but once granted, attackers gain access to personal information which is then leveraged to make phishing page popups launched by the OAuth app appear legitimate. The campaign targets businesses across the U.S. and Europe, including government agencies and healthcare institutions.

WithSecure Insight

This shows yet another method of abusing OAuth. In this case, the app itself requests minimal, read only permissions, however the data these permissions make available allows the attacker to generate a legitimate seeming phishing page. The attacker then uses the OAuth app permissions to cause that phishing page to appear as a pop-up for the victim, prompting them to enter their login credentials which can then be captured by the attacker and either used or sold on criminal forums.

Software supply chain

$1.5 billion ByBit hack was a software supply chain compromise

Further information on last month's $1.5Billion ByBit crypto theft has now been released. It appears that this was a software supply chain attack, where Safe{Wallet}, supplier of the cold wallet technology used by ByBit were compromised first.

The attackers successfully socially engineered a senior developer at ByBit, inducing them to download a malicious Docker container which they then executed on their work device. The attackers were then able to steal the developer's session token and use it to access Safe{Wallet}'s AWS environment, compromising their API key.

They then made a modification to the Safe{Wallet} code which would only affect transactions involving the targeted ByBit cold wallet. This modification caused the GUI to display the intended, authorised transaction, which was intended to be made, but in the background it actually emptied the wallet, transferring the funds to attacker-controlled accounts. The attackers made the code change 2 days before the successful transaction, then removed the malicious code 2 minutes later.

WithSecure Insight

The foundational principle of supply chain attacks is that any end point or product is reliant on a chain of other applications, functions, people, and services, and that they are only as secure as the weakest link in that supply chain. In this case the weak link turned out to be a senior developer who was willing to download and execute files sent to them over social media.

The attack was obviously well thought out and highly targeted, both because the initial compromise was one of very few individuals who had access to safe[wallet}'s API key, and because the changes that were made to the software would only take effect when the specifically targeted wallet was acted upon by the modified software. This attack employed social engineering, cloud, code, and cryptocurrency knowledge, and was likely a significant investment of effort by the attackers, however it is safe to say that unfortunately the investment appears to have paid off very well indeed.

SILK TYPHOON observed performing cloud supply chain attacks to access IT services, central and local government.

Silk Typhoon, a Chinese espionage group, has shifted tactics to perform cloud supply chain attacks. The group has been observed gaining access to victims through edge device exploitation and password brute force and discovery, then moving laterally into the cloud to access API keys and credentials associated with Privilege Access Management (PAM), Cloud app, and cloud data management companies. Once these upstream victims are compromised, they then target their tenants and customers, focusing on state, local government, and IT customers. Silk Typhoon are a well-resourced group who have used zero-day vulnerabilities in their attacks.

WithSecure Insight

The complexity of the cloud and the number of interrelated background services that make up each front-end service mean that it is ripe for supply chain attacks. This is another example of nation state APTs going after the supply chain of their victims, which does at least show us that it does require effort, investment, and expertise to perform such an attack.

Malicious NPM packages with embedded DPRK BeaverTail malware identified

North Korea's Lazarus Group has deployed six new malicious npm packages designed to steal credentials and deploy backdoors. As has been seen repeatedly before, the packages mimic trusted libraries and employ typo squatting tactics to deceive developers. The malicious packages contain embedded BeaverTail malware.

WithSecure Insight

Uploading malicious packages to repositories appears to be a well-established targeting and delivery method for multiple actors now. While the effectiveness of such attacks is unknown and questionable, it is definitely part of Lazarus Group's playbook, which indicates that they are most likely finding some success.

Annual summaries

French cyber agency ANSSI sees 2024 dominated by edge mass exploitation and software supply chain attacks

The French Cybersecurity Agency (ANSSI) has released its Cyber Threat Overview for 2024, detailing prevalent threats and pivotal incidents. The report details a year dominated by edge device exploitation and software supply chain attacks, often leading to ransomware attacks. ANSSI did note however that attacks against telecoms infrastructure was more likely to lead to espionage, not ransomware.

WithSecure Insight

ANSSI obviously have a very specific view of the cyber security landscape, being the French cyber security agency, however what they have observed very much lines up with our own assessment.

400% YoY increase in identity attacks observed by Red Canary

Red Canary's 2025 Threat Detection Report identifies their most commonly observed ATT&CK techniques. This year, the top techniques were cloud native identity-based attacks, with 4 times as many identity attacks observed this year as last year.

WithSecure Insight

Identity is a key battleground for cyber attackers and defenders, and this may in part be down to the effectiveness of endpoint XDR, and the breadth of cloud adoption. If services are accessible from the Internet, secured behind identity, then if you can steal/compromise that identity without deploying malware on an endpoint, you can bypass a significant proportion of the security defenses of most organizations.

33% YoY increase in credentials compromised in 2024

In Flashpoint's 2025 Global Threat Intelligence Report, Flashpoint stated that the volume of compromised credentials in 2024 increased by 33% YoY to over 3 billion, 75% of which came from Infostealer infections. Vulnerabilities increased 12%, and more than 39% of 2024 CVEs were found to have public exploit code available.

WithSecure Insight

Once again, this correlates with our own assessment and visibility. Infostealers are hugely popular with attackers as they are easily delivered, they don't need to maintain persistence, and the credentials that they steal can be easily monetized and sold on to other attackers. Even with MFA and advanced identity solutions, if credentials are compromised an attacker is a significant step closer to full account takeover.

In Brief

Microsoft identify members of multi-level LLM jacking operation Storm-2139

A hacking group known as Storm-2139 exploited exposed API keys to hijack Azure AI services, generating illicit content and bypassing built-in safety mechanisms.

Microsoft's digital crimes unit identified and named four individuals involved in what was a multi-level operation which involved compromising LLM hosting environments, creating tools which would be hosted on those environments, then selling access to services employing the tools to end users.

40% of cloud infrastructure networks allow any/any firewall access to at least one major cloud provider

Hackers are exploiting cloud misconfigurations to spread malware, with 40% of networks allowing 'any/any' access to at least one major cloud provider.

Malware including XWorm, Havoc, Sliver C2, and more have been observed using legitimate cloud services for malicious resources, whether creating their own projects or leveraging compromised accounts and environments.

This highlights the importance of properly securing networks by hardening firewall and cloud configurations.

UK NCSC warns of enterprise risks from adoption of TLS 1.3

The UK NCSC have released a statement about adoption of TLS 1.3. It states that adoption presents challenges for enterprise security by making it harder to inspect encrypted traffic or identify connection endpoints. This will prevent security appliances from determining the risk level of connections, and it will no longer be possible to partially proxy connections, as typically happens now. As such connections will have to either be un-proxied or proxied for the entire duration of the connection, which could have both security and privacy issues.

PHP-CGI vulnerability exploitation targeting UK and Spain observed from German IPs

An international attack campaign exploiting CVE-2024-4577, a critical PHP-CGI remote code execution flaw, has been detected by GreyNoise. The campaign, initially reported by Cisco Talos, targets Windows systems to deploy Cobalt Strike beacons and conduct post-exploitation activities using the TaoWu toolkit.

GreyNoise telemetry reveals widespread exploitation across multiple regions, including the United Kingdom and Spain, with over 1,089 unique IPs attempting exploitation in January 2025 alone. Organizations with internet-facing PHP-CGI installations are advised to block malicious IPs and perform retro-hunts to identify similar exploitation patterns.

Threat data highlights

Phishing malware delivery

During the month of March 2025, we observed a 268% uptick in sightings of malware delivered via e-mail across our telemetry compared to the month prior. However, this spike was largely driven by Snake Keylogger and Formbook malware campaigns. Snake Keylogger accounted for 39% of all sightings across the globe, while Formbook accounted for 23%.

In terms of geographically bound sightings, Formbook accounted for approximately 50% of sightings and GuLoader 20% across all continents, except for Asia and Europe. AgentTesla saw a global decline in terms of sightings except for Europe.

Europe saw a 30% rise in AsyncRAT sightings, while Asia saw a 23% increase in ValleyRAT sightings. Europe also saw a decline in MassLogger sightings with a 33-point decrease compared to the month prior.

The trend for lures employed in these sightings remained the same, with Supply Chain-related lures leading followed by financial and shipping lures, respectively.

Detection and response highlights

MDR

FakeCaptcha/ClickFix continues to be an extremely popular delivery method and was almost entirely observed being used for Infostealer delivery. Infostealer infections responded to were overwhelmingly Lumma infections, although AMOS (Mac) was observed. There were also some instances of RaspberryRobin infection, a malware that spreads through infected USB sticks.

Detection capability highlights

In March there were 352 modifications to detection rules across Windows, Linux, and Mac operating systems.

Notable new detections include:

- SMB Share enumeration
- Windows MSC file downloaded from the Internet
- Active Directory Certificate Services (AD CS) enumeration
- AD CS + Kerberos abuse
- MacOS defender tampering detection

IR

An incident occurred where a publicly exposed Remote Desktop Protocol (RDP) server and weak credentials allowed attacker access, leading to further system discovery and attempted lateral movement towards Domain controllers.

A publicly exposed legacy webserver for processing printing paper orders was exploited by an unknown threat actor using a weakly secured PIN code to place printing orders.

Investigation into an externally facing Geoserver where an unknown threat actor exploited a publicly known vulnerability on the Geoserver service to perform remote code execution.

NCSC case where ISP routers were compromised by SaltTyphoon threat actor group exploiting public facing software vulnerabilities on ISP router

Investigation into a malware outbreak related to a Monero cryptocurrency miner within a client's network environment.

About WithSecure™

WithSecure™, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies. Committed to the European Way of data protection, WithSecure™ prioritizes privacy, data sovereignty, and regulatory compliance.

Boasting more than 35 years of industry experience, WithSecure™ has designed its portfolio to navigate the paradigm shift from reactive to proactive cyber security. In alignment with its commitment to collaborative growth, WithSecure™ offers partners flexible commercial models, ensuring mutual success across the dynamic cyber security landscape.

Central to WithSecure's™ cutting-edge offerings is Elements Cloud, which seamlessly integrates AI-powered technologies, human expertise, and co-security services. Further, it empowers mid-market customers with modular capabilities spanning endpoint and cloud protection, threat detection and response, and exposure management.

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