WITH secure

Threat Highlight Report

April 2025

Table of Contents

Foreword 4

Monthly highlights 5

CVE program nearly shuts down, gets 11th hour funding approval from US government 5
Symlink backdoor detected on 16,000 Fortinet devices 6
TJ-Actions supply chain compromise began 2 steps further up software supply chain 7
Broadcom halts VMWare workstation auto updates without notice 8
SAP NetWeaver CVE-2025-31324 reportedly exploited as a zero-day, though SAP disputes this 9

Ransomware 10

April ransomware statistics 11
April ransomware victim volumes 13
New ransomware groups 15
European targeting 15
Ransomware news 16
DragonForce label themselves a cartel, offer Ransomware Platform as a Service 16

AI 17

Microsoft Security Copilot identifies 20 vulnerabilities in open-source bootloaders 17
ChatGPT-4.1 assessed to be 3 times more vulnerable to guardrail bypass than 4o 18
Slop squatting attacks target hallucinated software supply chains in AI generated code 19

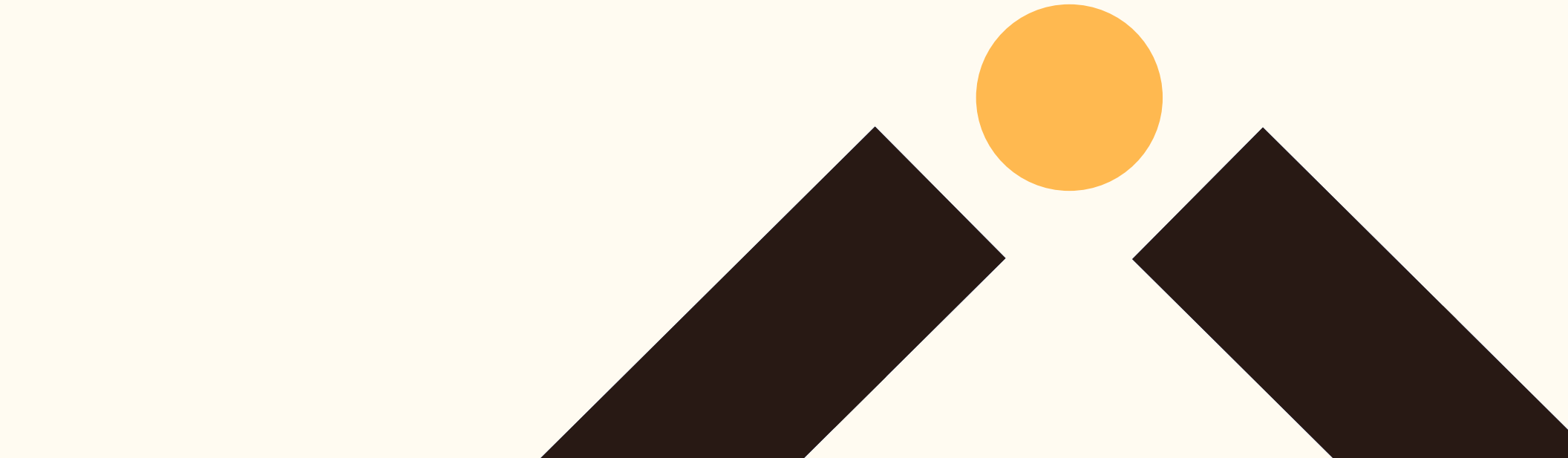
Cloud 20

WorkComposer employee monitoring app leaves S3 bucket of sensitive customer data and PII unsecured 20
Oracle privately admits to breach, but claims only an obsolete server was compromised, even as victims confirm production data was stolen 21

Identity 22

Gladinet CentreStack hardcoded private key vulnerability exploited 22
Flood of suspicious logins and transactions on Australian retirement fund portals, seemingly linked to stolen credentials 23

Annual summaries **24**
Talos IR Statistics see surge in abuse of valid credentials 24
Verizon IR statistics see increase in ransomware incidents, decrease in proportion of victims paying ransoms 24
IBM observe significant increase in phishing Infostealer delivery 25
VulnCheck find 28% of KEV CVEs exploited less than a day after publishing 26
Other highlights **27**
Cisco report a subset of Cisco devices are vulnerable to Erlang OTP SSH vulnerability 27
Ripple cryptocurrency library trojanized after developer account compromise 28
In Brief **29**
Threat data highlights **30**
Phishing malware delivery 30
Detection and response highlights **31**
IR 31
Detection capability highlights 31



Foreword

"Our lead story this month is the narrowly averted shutdown of the US government funded CVE database. Often, choosing stories for this report is based on whether they are interesting, important, or both. At first glance for many people this may have been considered both uninteresting and unimportant, but we believe otherwise, so much so that we did an entire podcast episode about it.

Several of our highlights this month are concerned with vulnerabilities and their exploitation, with a post-exploitation backdoor discovered on over 16,000 Fortinet network edge devices, and a SAP NetWeaver vulnerability which is being exploited at scale, and which WithSecure threat hunters have reported information on in a recently published blog post.

While April is often a quiet month for ransomware, the decrease in victims posted this month is particularly large, however this is mostly due to a significant drop in victims posted by C10p, possibly just because they have finished posting their victims from the Cleo mass exploitation campaign.

We have stories on AI, Cloud incidents, and Identity, as well as a brief roundup of the annual summaries published this month.

This month we have released two Cyber Threats Xposed podcasts. As mentioned above, one of those specifically focuses on the MITRE CVE program funding issues and the international fallout of that event. For this we are joined by Ben Moxon, WithSecure's head of Attack Surface Management and Exposure. Do check these out via your usual podcast channels."

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

Monthly highlights

CVE program nearly shuts down, gets 11th hour funding approval from US government

A near-defunding of the CVE program by the US Government raised significant concerns about the global reliance on US-based security initiatives. Although funding was eventually reinstated, the incident prompted the launch of competing CVE programs by other organizations. More widely, the situation has lead organizations to question the stability and reliability of other US government-funded security initiatives such as NVD and KEV.

WithSecure Insight

The CVE program ensures that there is a common language of CVE ID numbers for referring to software vulnerabilities, and that common language enables rapid and clear communication and coordination on the scale of adjacent desks in an IT support team, right up to international organizations and nation states. That communication and coordination is relied upon to ensure the best security efforts in the software supply chain of every organization or user. The issues that could arise without a central CVE ID database are quite clear to anybody who has ever had to try to navigate the chaotic naming conventions the cyber security industry uses to identify specific cyber threat actors, which sometimes seem to have as many names as there are security vendors. The almost-defunding of the CISA funded CVE program also brings up concerns about the NVD program, also run by CISA, which has been going through some quite public resourcing problems for a number of years now. These are programs relied upon internationally by the security and information technology communities, and it is disconcerting to find that these heavily relied upon programs may in fact not be that stable at all.

Symlink backdoor detected on 16,000 Fortinet devices

Shadowserver observed a symlink backdoor (originally reported earlier in the month by Fortinet themselves) on over 16,000 Fortinet devices.

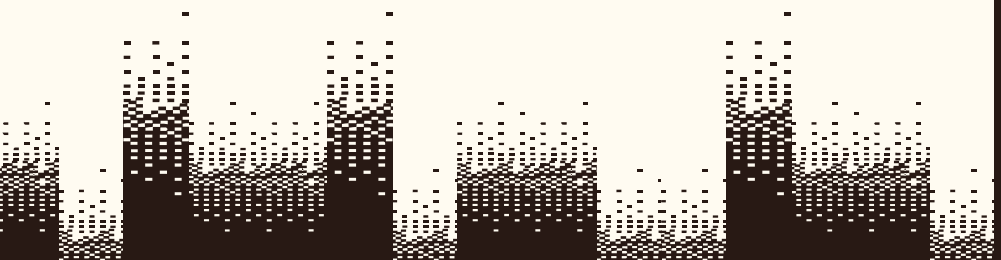
WithSecure Insight

This backdoor functions by simply creating a symlink in a publicly accessible location (in this case, the language files folder for the web UI) which points to “sensitive internal files”. It has not been reported which files were made accessible, but it may have been files containing local password hashes, for example. Several points make this campaign concerning:

- The fact that they are a type of device where the local file system is not typically directly accessed by administrators.
- The fact that while these devices may have been compromised by exploiting vulnerabilities, even if the vulnerability has since been patched, the backdoor will remain unaffected unless it is specifically and separately removed.
- The sheer number of devices known to have this specific backdoor file present.
- And finally, that the creation of a symlink file pointing in a public location, pointing to a sensitive private file, can be done on almost any web server.

TJ-Actions supply chain compromise began 2 steps further up software supply chain

Investigations into the TJ-actions supply chain attack have found that it originated from the compromise of another project called SpotBugs, which was itself included in reviewdog, a dependency of TJ-actions. This multi-step compromise allowed attackers to weaponize TJ-actions three months after initially compromising SpotBugs, indicating a strategic approach to maximize the impact of their access.



WithSecure Insight

Software supply chain compromises are of great concern as due to the nature of software supply chains they are difficult to identify and defend against, and they can affect many victims at once through a single compromise. This story highlights that compromises can happen any number of steps up the supply chain, and each step in that chain is an additional opportunity for an attacker to compromise a widely used and trusted piece of software.

Broadcom halts VMWare workstation auto updates without notice

Users of Broadcom VMWare Workstation report that they now face errors with the auto-update process. However, this does not seem to be due to a fault, but instead because Broadcom now require all users to login to the support portal before downloading any update files, forcing manual updates. This change has caused problems for users who relied on seamless automatic updates for security patches and bug fixes.

WithSecure Insight

Automatic updates are heavily relied upon to ensure that updates are distributed and applied as quickly as possible, so it seems counterintuitive to break that process. While it should be possible for future versions of VMWare workstation to be configured to store the required username and password and supply it when needed to logon to the Broadcom support portal, doing so could simply create yet another credential storage location that attackers could retrieve credentials from. This is not currently a concern however, as Broadcom have not commented on the change, or indicated that they will be changing VMWare Workstation to store credentials and perform auto-updates.

SAP NetWeaver CVE-2025-31324 reportedly exploited as a zero-day, though SAP disputes this

SAP patched the NetWeaver vulnerability CVE-2025-31324, but conflicting reports emerged regarding its exploitation as a zero-day. While SAP denied any evidence of zero-day exploitation or customer impact, multiple security vendors, including WithSecure, observed exploitation activities seemingly linked to this vulnerability as early as March, highlighting discrepancies in the reported timeline and severity.

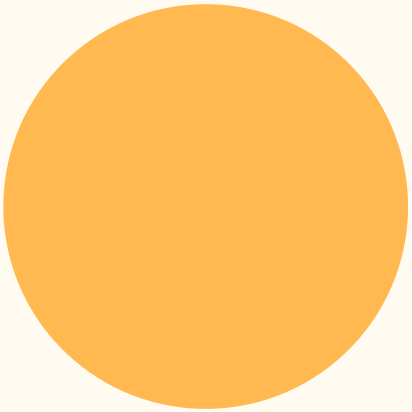
WithSecure Insight

NetWeaver is the basis of many of SAP's products, and SAP products are often used in large enterprise technology stacks. As such a widely exploited zero-day vulnerability in NetWeaver has the potential to have a big impact. While SAP say they have no evidence that a vulnerability has been exploited as a zero-day, it is possible that without fine grained logging at the very least it would be difficult to prove that this specific vulnerability has been compromised. While SAP and the wider security community may not agree entirely on some aspects of this situation, all commentators agree that this is a serious vulnerability in a commonly used enterprise software stack, and that organizations using NetWeaver should patch and investigate urgently. For specific details of the NetWeaver compromise detected and investigated by WithSecure, check the recent blog post by Rob Anderson.

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.



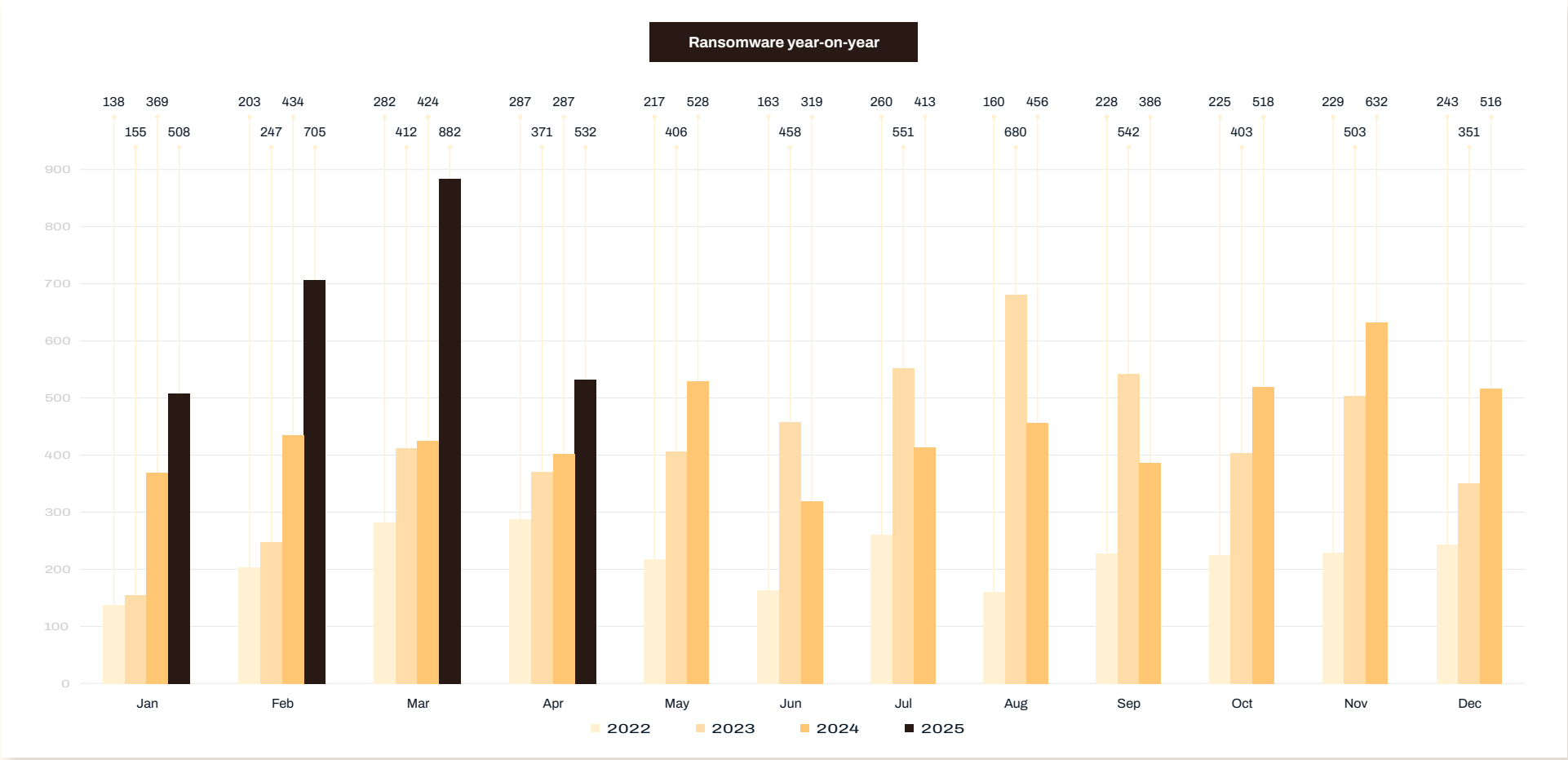
With this said, we can draw some insight from this data with sensible assumptions – and recognizing the data isn’t perfect, it does provide a decent gauge on the ransomware landscape. The assumptions the industry typically abide by are:

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

April ransomware statistics

April's numbers significantly fell from March's record totals, down from 882 to 532. This is largely driven by a cessation in C10ps victim posting from the Cleo campaign. Curiously, RansomHub's victim posting count fell from 88 to Zero. Furthermore, April's numbers have always been lower than March's. Sharp drops in victim postings from Fog (-32) and Frag (-26) also contributed to the 350 drop in victim postings this month.

As with March, Babuk numbers have been excluded from total counts as we do not have confidence in the accuracy of their claims.




12 MONTH VOLUMES
1000
900
800
700
600
500
400
300
200
100
0
528
319
413
456
386
518
632
516
508
705
882
532
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
Nov-24
Dec-24
Jan-25
Feb-25
Mar-25

April ransomware victim volumes

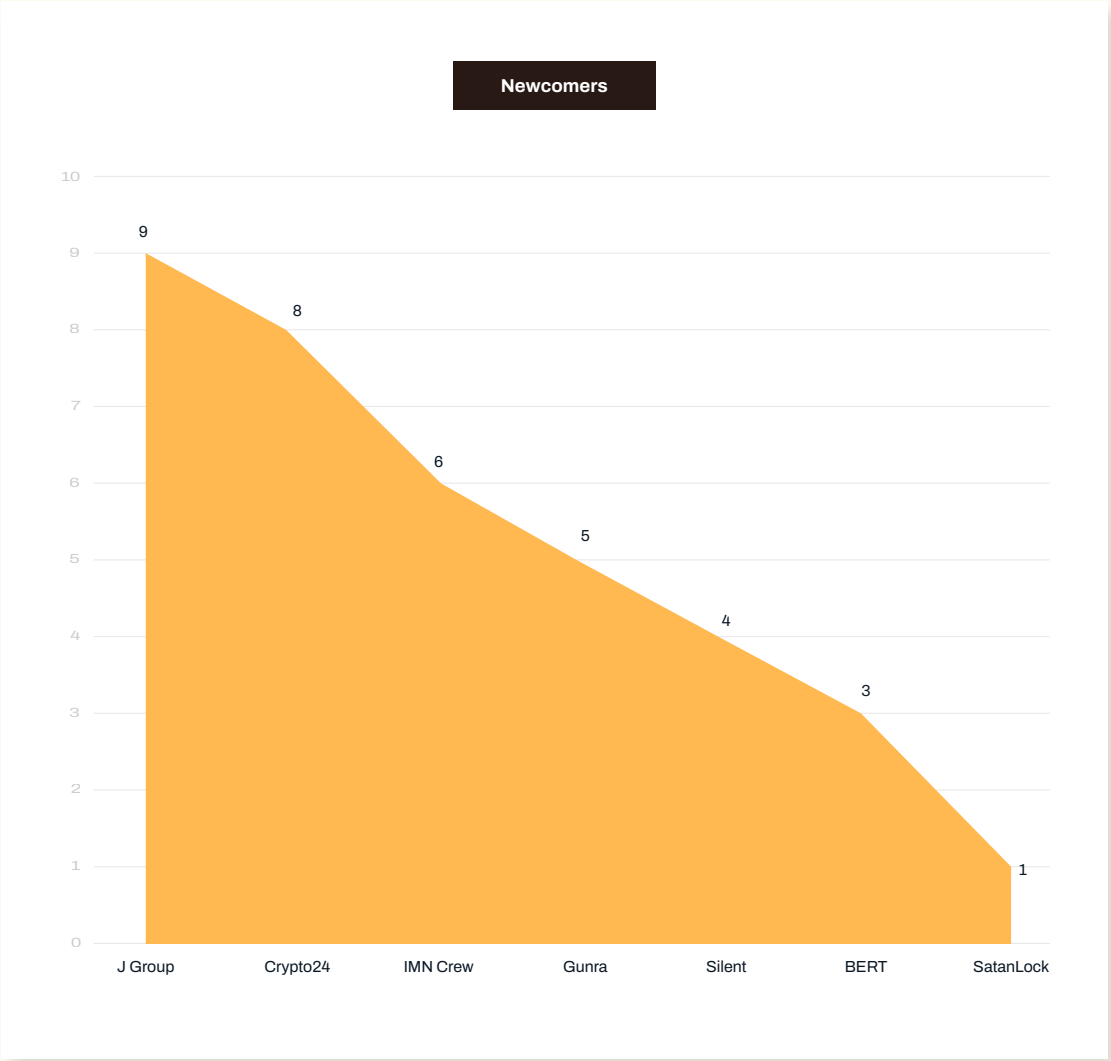
Top 20 April			
Leak Site	**March**	**April**	**Delta**
Qilin	47	75	28
Akira	68	67	-1
Play	31	50	19
Lynx	30	31	1
LeakedData	23	24	1
NightSpire	16	21	5
Safepay	42	20	-22
DragonForce	15	20	5
INC Ransom	30	19	-11
BABUK 2.0*	94	17	-77
Kill Security	20	17	-3
Hunters International	6	17	11
Medusa	18	14	-4
Sarcoma	10	14	4
LockBit	4	13	9
RALord	5	11	6
Rhysida	8	9	1
J Group	-	9	9
Crypto24	-	8	8
INTERLOCK	6	7	1

Biggest Risers			
Leak Site	**March**	**April**	**Delta**
Qilin	47	75	28
Play	31	50	19
Hunters International	6	17	11
LockBit	4	13	9
J Group	-	9	9
Crypto24	-	8	8
RALord	5	11	6
IMN Crew	-	6	6
NightSpire	16	21	5
DragonForce	15	20	5

Biggest Fallers			
Leak Site	**March**	**April**	**Delta**
CL0P	217	3	-214
RansomHub	88	0	-88
BABUK 2.0*	94	17	-77
Fog	32	0	-32
Frag	27	1	-26
Safepay	42	20	-22
Arcus Media	15	0	-15
BianLian	12	0	-12
INC Ransom	30	19	-11
CrazyHunter	10	0	-10

New ransomware groups

There were 7 new ransomware data leak sites (DLS) observed this month posting a total of 36 victims. There were no immediately discernible patterns from any of the known victims of the ransomware newcomers.



European targeting

17.54% of victims were based in the EU this month. The following represents the ransomware brands that disproportionately impact victims in the EU.

SAFEPAY have an unusually large European proportion of victims this month, primarily due to a large number of German victims (11 out of 20).

DLS	% EU
SAFEPAY	60
Hunters International	41.18
INC Ransom	31.58
NightSpire	28
RALord	27.27
Akira	24.64
Sarcoma	21.43
Kill Security	18.18
Qilin	18.18

Ransomware news

DragonForce label themselves a cartel offering a Ransomware Platform as a Service

DragonForce has rebranded itself as a “Cartel” and shifted to a distributed “Ransomware Platform as a Service” model. This new approach allows affiliates to white-label DragonForce’s tools and infrastructure, creating their own “Brands.” Affiliates are offered services like file storage, server monitoring, and negotiation tools, democratizing access to ransomware and potentially increasing the number of threat actors. DragonForce affiliates already appear to have had some high-profile successes, having claimed the compromise of UK retailers Harrods, Marks and Spencer, and Co-op. An alleged DragonForce spokesperson provided proof of compromise of Co-op to the BBC, but did not provide any proof for the other retailers. Some reports state that actors under the Scattered Spider umbrella performed these compromises, but this reporting remains vague.

WithSecure Insight

Any innovation in the ransomware industry is of concern, as it has the potential to affect the volume, success rate, and severity of attacks. We have noted previously that evolution in the ransomware industry is often due to outside influences, and that also seems to be the case here. The 2024 ransomware landscape was dominated by the take down of Lockbit and the exit scam of ALPHV. In response to those events RansomHub and several other brands launched which offered more control to affiliates. Now, DragonForce have launched, which seemingly intends for affiliates to fully operate under their own brands, simply using DragonForce’s ransomware platform. This provides more control to affiliates, but DragonForce may also be hoping that letting affiliates operate under their own brands, instead of the DragonForce umbrella may cause law enforcement disruption operations to focus more on the affiliates and less on the central brand. As such it is interesting that DragonForce have been linked to the compromises of multiple UK retailers this month, and through that to Scattered Spider, as the Scattered Spider designation is itself incredibly vague, being more a culture and collection of TTPs, than an actual group of actors.

AI

Microsoft Security Copilot identifies 20 vulnerabilities in open-source bootloaders

Using Microsoft Security Copilot, researchers at Microsoft identified 20 vulnerabilities in GRUB2, U-Boot, and Barebox bootloaders, including an exploitable integer overflow. These vulnerabilities could allow attackers to bypass UEFI Secure Boot, install persistent malware, and gain complete control over devices, posing significant threats to enterprise environments. Microsoft note that the use of Security Copilot saved them roughly 1 week of researcher time.

WithSecure Insight

It is always good to hear of positive uses for LLMs, and from this report it does seem like this could be a good use case for LLMs as the outputs from the LLM are specific security vulnerabilities and development problems, the existence of which can be verified. While Microsoft do state that this saved 1 week of time, they don't state how much time was spent on the task in total, however they do state that the LLM initially reported 5 issues in GRUB2, 3 of which were false positives, 1 of which was unexploitable, and 1 of which was legitimate, giving only a 20% success rate. After verifying the actual vulnerability, Copilot was then prompted to identify other similar patterns in the code base. This output was then once again reviewed and verified by researchers, although the false positive rate was not given for this step of the process.

ChatGPT-4.1 assessed to be 3 times more vulnerable to guardrail bypass than 4o

Security researchers at SplxAI found that GPT-4.1 is three times more likely to bypass security safeguards and allow intentional misuse compared to its predecessor, GPT-4o. The lack of a safety report for GPT-4.1 raises concerns about its vulnerability to off-topic responses and intentional misuse.

WithSecure Insight

While it is widely acknowledged (even by OpenAI themselves) that the ChatGPT version numbering system is terrible, there is always great excitement over the release of a new version of the service. However, that excitement is down to the belief that newer versions will be better in multiple ways that matter. While the LLM industry in its current form does not have much history to compare to, it is still very unusual that they have apparently released a product which could be described as 3 times more vulnerable to attacks.

Slop squatting attacks target hallucinated software supply chains in AI generated code

An attack dubbed Slop Squatting exploits the tendency of AI-generated code to invent non-existent package names, allowing attackers to predict and hijack these phantom packages to insert malicious code. This method poses a significant risk to the software supply chain, as AI code assistants frequently hallucinate package names, leading to potential security breaches.

WithSecure Insight

While the name of this attack is quite off putting, it is an example of some very excellent security lateral thinking. We are well aware that LLMs hallucinate plausible yet incorrect output, and that this can occur when generating code, resulting references to non-existent resources. However, the researchers here recognized that the non-existent libraries and resources which LLM-generated code invents are predictable and so can be pre-registered and squatted. This hammers home yet again the fact that LLM output that needs to be correct and trusted, instead of simply plausible, must be checked and verified before use.

Cloud

WorkComposer employee monitoring app leaves S3 bucket of sensitive customer data and PII unsecured

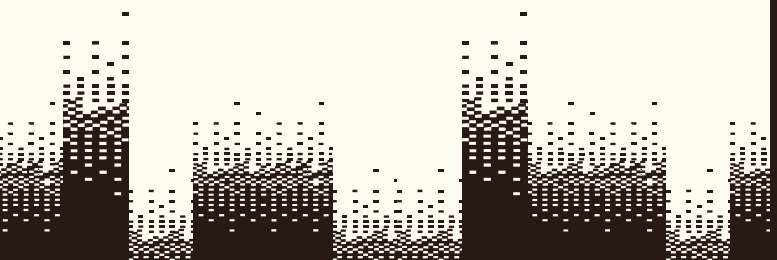
Data from the employee monitoring app WorkComposer was left in an unsecured Amazon S3 bucket, exposing over 21 million screenshots of enterprise activity. The leaked data includes sensitive information such as login pages, credentials, and confidential business documents, posing severe privacy and security risks for businesses which are customers of WorkComposer.

WithSecure Insight

Leaving back-end resources unsecured is a classic security blunder for cloud-based services. It is likely that this data was accessed via an API front end which would almost certainly have implemented standard security practices (such as requiring some form of authentication), however that because the back end was not secured, it was possible to entirely bypass those security requirements. The nature of the service and the type of data it relied upon means that large amounts of sensitive information covering every facet of the operation of WorkComposer's customers was publicly available to anyone who cared to look for it.

Oracle privately admits to breach, but claims only an obsolete server was compromised, even as victims confirm production data was stolen

Oracle privately notified customers about a breach involving obsolete servers, denying that the Oracle Cloud Infrastructure (OCI) was compromised. However, reports indicate that the breach led to the theft of production data and customer password hashes, raising concerns about the security of Oracle's cloud services.



WithSecure Insight

This incident rather unfortunately serves as a classic example of how not to do incident communication. Before Oracle admitted to any incident, multiple of their customers had confirmed that their data, which had been stored on Oracle cloud servers, had been stolen. However, they had no information as to how it had been stolen, or where from, or how much more data might have been illegally accessed. When Oracle did finally make a statement confirming there had been an incident, it appeared to be carefully worded to state that there had not been a breach of Oracle Cloud Infrastructure. However, Oracle Cloud Infrastructure is a brand name for a service Oracle offers, and they appear to have been able to make that claim because the server which was compromised was not defined as part of that service/brand, by Oracle themselves. Unfortunately, while Oracle did not define it as such, it still provided the threat actor with access to live data from customer production environments hosted on Oracle Cloud Infrastructure, including hashed credentials.

Identity

Gladinet CentreStack hardcoded private key vulnerability exploited

A critical vulnerability, CVE-2025-30406, in Gladinet CentreStack is being actively exploited in a campaign with infrastructure overlap with the KrustyLoader ScreenConnect exploitation campaign reported by WithSecure in early 2024. This vulnerability stems from a hardcoded ASP.NET MachineKey, allowing threat actors to serialize payloads for server-side deserialization, leading to remote code execution. The patch method has been described as having certain complexities which cause confusion about whether devices are being patched correctly.

WithSecure Insight

This is the second story in recent months relating to hardcoded ASP.NET machine keys, something which most people probably have not considered before. Essentially, these machine keys are cryptographic identities which a server can use to identify itself in a server farm for example. As such, if a threat actor has access to a machine key they can perform certain actions as if they were the server.

Flood of suspicious logins and transactions on Australian retirement fund portals, seemingly linked to stolen credentials

Multiple Australian retirement fund portals experienced a surge of suspicious logins and transaction attempts, indicating a coordinated campaign by threat actors who likely acquired correct credentials from infostealer logs. While some funds have publicly stated that no members' funds were accessed, others have privately stated that hundreds of individuals' pension funds saw unauthorized withdrawals.

WithSecure Insight

While it is currently unclear what caused this flood of unauthorized logins and transactions, it seems very likely that an actor identified that credentials for certain domains could provide highly valuable access, and that they then gathered logins from infostealer logs for this campaign. This is one of the dangers of the infostealer log marketplace, there are huge numbers of credentials which have been stolen, and until an attacker puts them to use then the original owner may not even know they have been compromised. This is the value of passkey authentication and MFA, as when implemented correctly they ensure that the true owner of the account (or at least whoever has access to the MFA or passkey) must approve any login. Unfortunately, in this case it seems that some of the pension portals used email as the MFA vector, and of course if an infostealer was able to steal the login to a user's pension portal, it is very likely that it was also able to steal the login to their email account.

Annual summaries

Talos IR Statistics see surge in abuse of valid credentials

Talos observed that when the method was known, 69% of initial access was through valid credentials. While MFA could have protected against this, in 65% of incidents MFA was not implemented correctly, or was only partially enabled.

WithSecure Insight

This aligns with WithSecure observations about the importance of Identity security.

Verizon IR statistics see increase in ransomware incidents, decrease in proportion of victims paying ransoms

Verizon IR data, while heavily US focused, found a significant increase in the volume of ransomware cases in 2024 but only 36% of victims paid ransoms, down from 50% in 2023. The report also noted a 34% increase in exploited vulnerabilities.

WithSecure Insight

This adds additional observations to the current body of data about the effectiveness of the ransomware industry. In 2025 there have been a number of reports that have suggested that while the number of ransomware incidents has increased, the total amount paid in ransoms has decreased. There has been speculation as to whether this was caused by a general change in targeted, with attackers focusing on smaller organizations and smaller payments, or if there was a drop in payment rates.

IBM observe significant increase in phishing Infostealer delivery

In 2024 IBM observed an 84% increase in weekly average infostealer delivery via phishing emails. So far in 2025 that volume is even greater, with a 180% increase from 2023 levels. Credential harvesting occurred in 28% of IR cases in 2024, and the top IAVs were valid credentials and public service exploitation, at 30% of incidents each.

WithSecure Insight

There are multiple data points in IBM's data which once again highlight the growing threat of identity-based attacks. Infostealers delivered by phishing emails have been around for a very long time, they are not a new threat, and yet according to IBM's data here the volume and the threat is growing rapidly. As such, it is likely that this almost old-fashioned type of attack has found a new lease of life thanks to the behavior of the victims of these attacks and the huge growth in cloud dependent, hybrid environments where user identity, rather than the network perimeter, is key.

VulnCheck find 28% of KEV CVEs exploited less than a day after publishing

A recent report analyses known exploited vulnerabilities (KEVs) disclosed in Q1 2025, revealing that 28.3% of KEVs had exploitation evidence disclosed in less than a day of a CVE being published. The top categories associated with new KEVs were Content Management Systems, Network Edge Devices, and Operating Systems, with Microsoft Windows and Broadcom VMware being the leading products impacted. The analysis of NVD/CVE statuses of KEVs identified gaps in NIST's NVD coverage, with 25.8% awaiting analysis. Furthermore, the report suggests that EPSS scores are largely a trailing indicator rather than a predictive tool for emerging threats, advising caution when relying on vulnerability scoring systems.

WithSecure Insight

We have discussed before that vulnerability exploitation against edge network devices is one of the primary methods of initial access for threat actors. This research illustrates the speed with which new vulnerabilities are being targeted, and the speed with which defenders need to respond. The highlighted gaps in NVD coverage also tie into the questions raised regarding the US funding of the CVE database program, as covered in our main highlights this month.

Other highlights

Cisco report a subset of Cisco devices are vulnerable to Erlang OTP SSH vulnerability

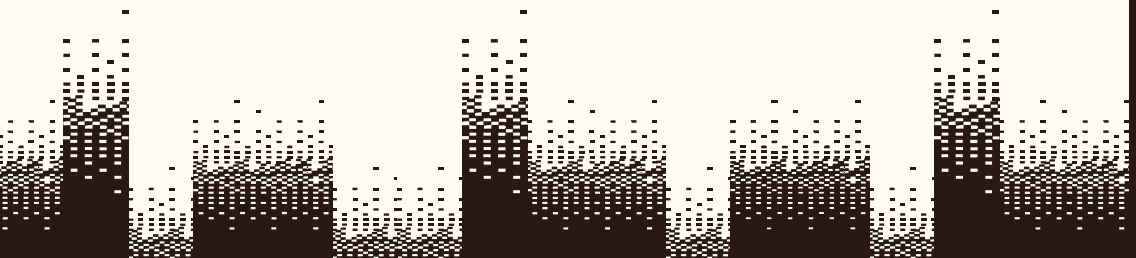
Cisco reported that some of their devices are vulnerable to the Erlang OTP SSH vulnerability, CVE-2025-32433. This critical flaw allows unauthenticated remote attackers to perform remote code execution by exploiting improper handling of SSH messages during authentication. Cisco is still investigating which products are affected, but the vulnerability impacts critical infrastructure components, with proof-of-concept exploit code already circulating.

WithSecure Insight

Cisco of course have a huge market share of network devices, but what exactly does it mean that “some” products are affected? Well in 2018 (which was admittedly 7 years ago), Cisco stated that 90% of the devices across which Internet traffic transits ran Erlang OTP SSH, so unless that percentage has changed drastically in the last 7 years then this could be quite a significant issue.

Ripple cryptocurrency library trojanized after developer account compromise

A Ripple Cryptocurrency xrpl.js NPM package was backdoored to steal private keys, seemingly through compromise of a developer account. The malicious version was live for less than a day, but it sees more than 135,000 downloads per week. The backdoor was introduced by a user named “mukulljangid,” likely a Ripple employee whose npm account was hacked. The malicious code was designed to exfiltrate private keys to an external domain.



WithSecure Insight

Yet again a software supply chain compromise is used to specifically target cryptocurrency technologies and users. It is unclear just how many users could have been affected by this compromise, as not only were there potentially 10-20,000 downloads of the library from NPM, but these downloaded packages could well have been included in software that was then distributed further. The only silver lining is that it does at least appear that the compromise was of this package directly, rather than of some other dependency even higher up the supply chain.

In Brief

99% of enterprise users have at least 1 browser extension installed, and 53% of extensions can access sensitive data such as cookies, passwords, page contents and browsing history, yet 54% of extension developers are identified only by a Gmail account.

Law enforcement Op Endgame, which previously took down many malware loader servers, has now detained 5 individuals who were customers/users of SmokeLoader. Europol report that some of the individuals have agreed to co-operate, and the investigation is ongoing.

This year Microsoft will begin blocking ActiveX content in Microsoft 365 and Office 2024, due to how heavily and persistently it is abused by attackers.

The December 2024 ransomware incident at Fourlis (an operator of IKEA stores in Eastern Europe) cost EUR20 million in sales, not including remediation costs.

Microsoft is to begin to offer hot patching for Windows Server 2025, but only as a paid for premium subscription.

Seemingly in response to US law enforcement disruption efforts, DPRK's fake IT worker campaigns seem to have refocused on European companies.

It appears that data from both Samsung Germany and UK Royal Mail was stolen from Spectos, a third-party logistics software supplier used by both companies.

UK Retailer Marks and Spencer experiences over a week of disruption after a DragonForce ransomware attack, reportedly linked to Scattered Spider/Oktapus.

Ransomhub RaaS group appears to have folded due to internal conflict, many affiliates appear to have moved to Qilin and DragonForce

A phishing campaign targeting Japanese online stock trading accounts resulted in $300 million of shares being sold, and the equivalent value in Chinese based shares being purchased.

Researchers find that AI powered spear phishing is now 24% more effective than human powered spear phishing.

Threat data highlights

Phishing malware delivery

Overall, the observed volume of malware delivered via e-mail across our telemetry remained similar in April 2025 compared to the month prior, with only a 7% increase.

Delivery of Formbook via malicious e-mail continued to rise, accounting for 32% of all sightings across the globe compared to 23% for the previous month. This was largely driven by sightings across Europe, which accounted for 72% of all Formbook sightings.

Delivery of Snake Keylogger via malicious e-mail decreased - while in March 2025 it accounted for close to 40% of all sightings across the globe, it only accounted for 11% of sightings in April 2025. Contrary to this wider trend, Asia saw a 24% increase in Snake Keylogger sightings this month.

Mass Keylogger accounted for 30% of all sightings across the globe in April 2025. This was reflected across all continents, except once again for Asia, which did not experience a noteworthy rise.

Remcos RAT sightings increased slightly in most continents except for Asia and Europe, contributing to approximately 20% of malware sightings per continent.

The trend for lures employed in these sightings remained the same, with Supply Chain-related lures being the most common, followed by financial, and then shipping lures.

Detection and response highlights

IR

Incident Response were engaged to investigate and remediate the following incidents:

The successful exploitation of a CrushFTP server via exploitation of CVE-2025-31161 occurred, leading to enumeration and exfiltration of the configuration multiple times, along with signs of multiple remote access tools and C2 frameworks being dropped. As such it is highly likely that multiple threat actors, likely IABs, were active on the compromised device.

A threat actor used valid credentials to connect to an enterprise VPN which was not protected with MFA. After this, the threat actor moved laterally and deployed an SSH reverse proxy on two hosts, later exfiltrating SAM registry hives, most likely to perform offline brute force attacks.

Detection capability highlights

In April there were 359 modifications to detection rules across Windows, Linux, and Mac operating systems.

Notable new detections include:

- Additional Async RAT behavioral detections
- Suspicious use of certificates for Kerberos TGT request and logon
- Cryptowallet file access by python
- Suspicious downloads by SQL server
- Impacket lateral movement detection

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.