

Threat Highlight Report

May 2025

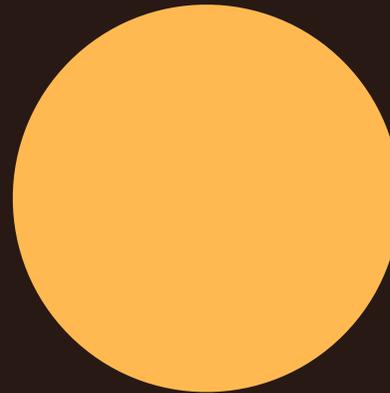


Table of Contents

Foreword	4
Monthly highlights	5
Details of Scattered Spider social engineering spree.....	5
Commvault have an extremely bad month	7
ConnectWise compromised, customer instances accessed	8
Trojanized KeePass steals credentials, results in ransomware.....	9
Ransomware	10
May ransomware statistics	11
May ransomware victim volumes	13
New ransomware groups.....	15
European targeting.....	15
Ransomware news	16
Lockbit hacked, site database published	16
Ransomhub ceases operations	16
FBI warn of vishing against legal sector	17
Identity	18
Japanese share trading compromises expand dramatically	18
89 million steam users records and logs of MFA access codes offered for sale.....	19
Exposed xAI private key grants ability to query and modify unreleased LLM models	19
Other highlights	20
Additional SAP NetWeaver zero-day identified and patched	20
Multiple LLM models prevent their own shutdown, even when instructed not to.....	21
Researchers detail multi platform cloud attacks using NPM package.json files	21
APT41 attributed malware observed using Google Calendar for C2 comms	22
In Brief	23
Threat data highlights	24
Phishing malware delivery	24

Foreword



“ This month has seen a mixture of both thematically and technologically linked cyber-incidents. Multiple UK high street retailers were compromised by Scattered Spider associated attackers engaging in ransomware attacks.

Those same attackers are reported to have then turned their attention towards the US retail sector.

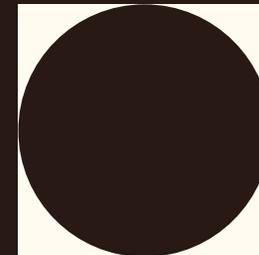
Both Commvault and ConnectWise appear to have been compromised, leading to the compromise of their customers also, however communications about these two situations remain unclear.

Regarding ransomware, this month there is good news as for the first time since September 2024 the number of victims posted to leak sites is lower than this same month last year.

At the same time there has been a lot of turbulence in the RaaS industry, with RansomHub, the highest volume group for the last 6 months seemingly ceasing operations, while Lockbit's data leak site (DLS) has been hacked, and the site data leaked by unknown attackers.

This month in the podcast we discuss these major stories, and we explain just what should make the UK retail sector attacks so interesting to those of us who do not work in or rely on the UK retail sector. ”

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



Monthly highlights

Details of Scattered Spider social engineering spree

In April it was disclosed that multiple UK retailers were compromised to various extents by ransomware actors [deploying the DragonForce ransomware locker](#). In May more details have come to light. Marks and Spencer and Co-Op were both compromised on the 22nd of June by actors believed to be associated with the very loose association of actors known as Scattered Spider, who deployed the DragonForce ransomware locker. M&S suffered more extensive damage, while Co-Op were able to mitigate the impact by physically unplugging servers to prevent encryption (Something that the attackers complained about in messages to journalists). M&S have stated that their cyber insurance is expected to cover £100 million of the impact, but that at present they expect the incident to cost them at least £300 million, or one third of the previous year's profit. On 1st of May, Harrods of [London disclosed that they too had been targeted](#) by an attempted compromise, but that they had been able to defend their networks without any noticeable disruption to their operations.



On the 6th of May the UK Legal Aid agency (The body responsible for public funding of legal representatives in UK courts for those who cannot afford them) then disclosed that [they too had experienced a cyber incident](#). This incident was first identified by them on the 23rd of April, at almost the same time as the M&S, Co-Op and Harrods incidents, and led to the theft of extensive PII on legal aid applicants, including domestic abuse survivors, with employment, criminal, and financial histories for applicants who applied as far back as 2010 stolen. One week later on the 14th of May, Peter Green Chilled, a regional cold chain storage and logistics company which supplies every major UK supermarket [also experienced a ransomware attack](#). On the 21st of May, Reuters reported that a source had informed them that the M&S attackers leveraged compromised accounts of Tata Consulting Services (TCS), a third-party contractor that manages some M&S systems. This has not been confirmed by M&S or TCS, however M&S confirmed that the attackers targeted a third party with a social engineering attack in order to gain access to the M&S network. Shortly after that TCS stated that they had begun an internal investigation to determine whether they were the source of the attack.

WithSecure Insight

When two organizations in the same sector and geography announce major cyber incidents within a short time frame, our first thought is always “Could these be linked?”. After the third event, the question becomes “How are these linked?”. Victims could be linked by their use of the same piece of industry specific software that an attacker has identified a vulnerability in, or by a shared service supplier. While it is not confirmed that TCS were the up-supply chain victim in these retail sector attacks, it is known that they provide IT managed services to both Co-op and M&S. Indeed, one of the systems that M&S specifically stated was heavily impacted by the attack was their customer loyalty program, a system which TCS implemented for the, and has since managed. TCS are an extremely large MSP with many customers, so it is interesting that the victims were within the same sector and geographical location. This can however be explained by the apparent social engineering aspect. A method commonly used in Scattered Spider TTPs is simply calling up users or support desks and simply asking them to do things.

Scattered Spider operators are known to be predominantly based in the US and UK, with English as a first language, which makes it easier to target organizations in those countries and would also make it easier to pretend to be an employee of UK or US based organization when calling a call center operated by people for whom English is not a first language. TCS are an Indian head quartered company, and it is highly likely that their call centers are based in India.

While we do not yet know if the UK Legal Aid attack is linked, the timing is extremely suspicious, and it is entirely possible that they are also customers of TCS, who as a low-cost MSP have many government contracts. While the Peter Green Chilled incident is also not known to be related, it would absolutely be possible that it is related. When an organization is compromised and data is stolen, it is common for attackers to then target suppliers and customers of the first victim, either with messages from compromised accounts and mailboxes, or in attacks which use compromised inside information to appear legitimate. While this campaign may only have directly impacted the UK, [Google issued a warning](#) in mid-May that they have observed the operators behind this attack turn their attention towards the US retail sector, using very similar social engineering tactics targeting IT help desks. This form of social engineering has been shown to be effective in many previous attacks, however this campaign has showed that the retail sector, and companies with outsourced tech support help desks may be particularly vulnerable.

Commvault have an extremely bad month

At the beginning of May two separate researchers identified that the maximum severity unauthenticated RCE vulnerability in Commvault Command Centre, CVE-2025-34028, was still exploitable even after applying the patch that was supposed to protect against it. This then turned it from an n-day with a patch available to a zero-day with no patch available.

Vulnerabilities are, unfortunately, relatively run of the mill, however later in the month CISA issued an advisory warning that threat actors are targeting Commvault instances hosted in Commvault's Azure cloud environment, stealing M365 tokens from the backup data and using them to access the customer M365 environment and in some cases more laterally to other systems from there. The attackers were seemingly exploiting CVE-2025-3928, a vulnerability originally disclosed and patched in February that allows but it is unclear whether this activity occurred prior to the patch being available, or if the vulnerability remained exploitable in the cloud hosted instances, or whether the attacker exploited it for initial access, then was able to maintain access after it was patched. CISA warn that they believe this activity to be part of a larger campaign targeting SaaS cloud applications with overly permissive default configurations and elevated permissions.

WithSecure Insight

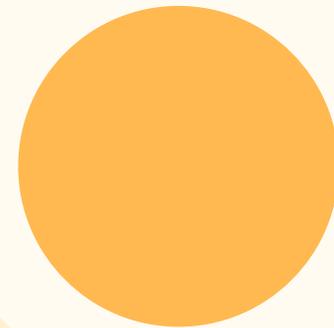
SaaS applications can provide organizations with managed, hosted critical services at a very low administrative overhead to the organization. These services can be made available to users and offices around the world and will always be automatically updated to the latest version. That is the promise at least. However, they are also excellent sources of valuable data and credentials for attackers. The benefit to an attacker of compromising a SaaS hosting environments is the access it provides to all of the tenants/customers of that environment, and their individual instances. In this case, those instances contained backed up data, and that data contained additional tokens which allowed access to other SaaS environments. Cloud services are highly accessible and highly valuable, and as such need to be robustly and comprehensively defended by both tenants and service providers.

ConnectWise compromised, customer instances accessed

ConnectWise have issued an advisory stating that their internal systems were compromised by a nation state actor which accessed the ScreenConnect instances of a small number of customers. They state that the attacker used the access to the ScreenConnect hosting environment, and CVE-2025-3935 in ScreenConnect to access customer instances. This vulnerability is the use of ASP.NET machine keys to protect the ViewState. This means that if an attacker has privileged access to the hosting server, they can access the machine key, then send their own malicious ViewState to the hosted website, potentially leading to remote code execution. ScreenConnect state that no further malicious activity has been identified since the patch was issued in April, and that all affected customers have already been contacted directly and notified.

WithSecure Insight

This is similar to the previous Commvault story, but in this case ConnectWise themselves were compromised. The use of the vulnerability here is unclear, as the attackers needed to have privileged access already in order to abuse it, however it may be that they had privileged access to a hosting server, but that they would not have been able to interfere with hosted instances of the application without this vulnerability. The public communications about this incident have not been particularly clear, and ScreenConnect have published very little information about what occurred. They have at least stated however, that they have directly contacted all customers who they know to be affected.

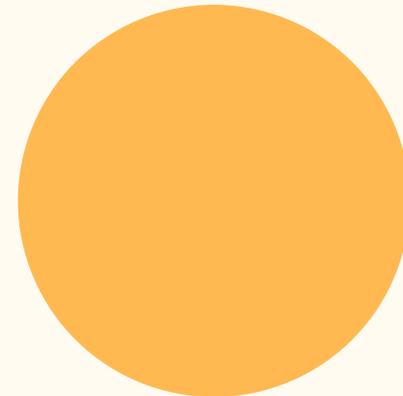


Trojanized KeePass steals credentials, results in ransomware

[WithSecure researchers have identified a campaign](#), most likely by UNC4696 which distributed trojanized KeePass installers over at least 8 months, using them to steal credentials and install Cobalt Strike. The attacker appeared to be an Initial Access Broker (IAB), and in a case investigated by WithSecure IR the initial compromise via the Trojanized KeePass was later followed by the deployment of ransomware on ESXi servers, most likely by attackers who purchased the access from the IAB. In a particularly cunning twist, the trojanized KeePass binary would exfiltrate the credentials from any KeePass database it was used to open. The campaign also appears to have distributed trojanized versions of other software using SEO optimization and a wide array of imitation hosting websites and advertisements.

WithSecure Insight

This case underscores the risks of trusted software being hijacked and weaponized. It is extremely common for users to simply open a search engine and search for a piece of software they want to download. Attackers know this, and for a long time have been known to create fake websites and download links offering malware disguised as trusted, legitimate software. This is the first instance that WithSecure are aware of where the source code of legitimate software has been modified to deliberately perform multiple additional malicious operations, as well as the expected, legitimate activity.



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:



Extortion success is another key factor, if the amount of paying victims greatly increases, 'total' ransomware numbers may also appear to decrease.



It is attacker led, and some attackers may be incentivized to post incorrect data.



It is fluid, and victims are added and removed frequently.

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:



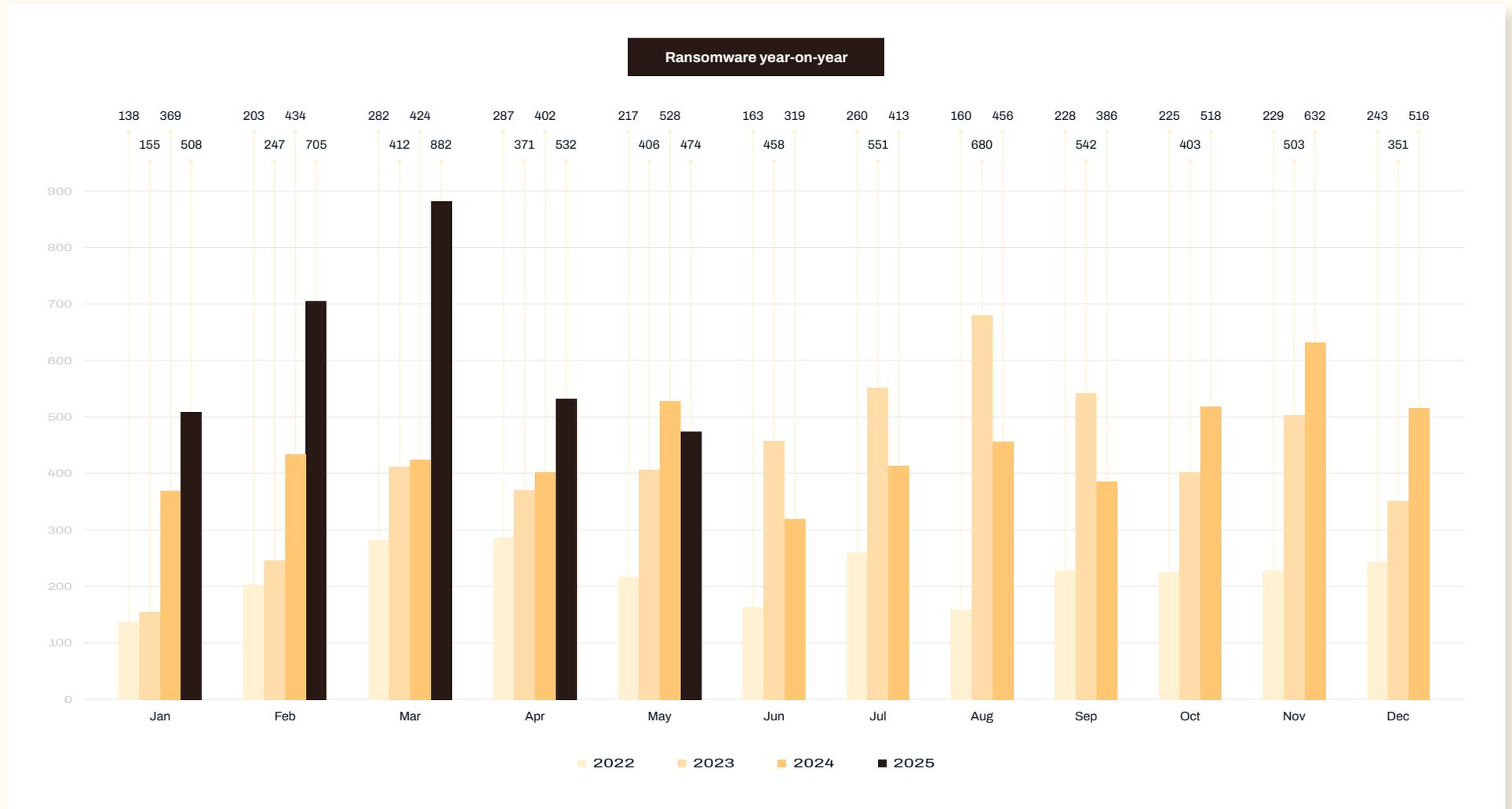
There is a roughly relatively consistent month-on-month victim payment rate.



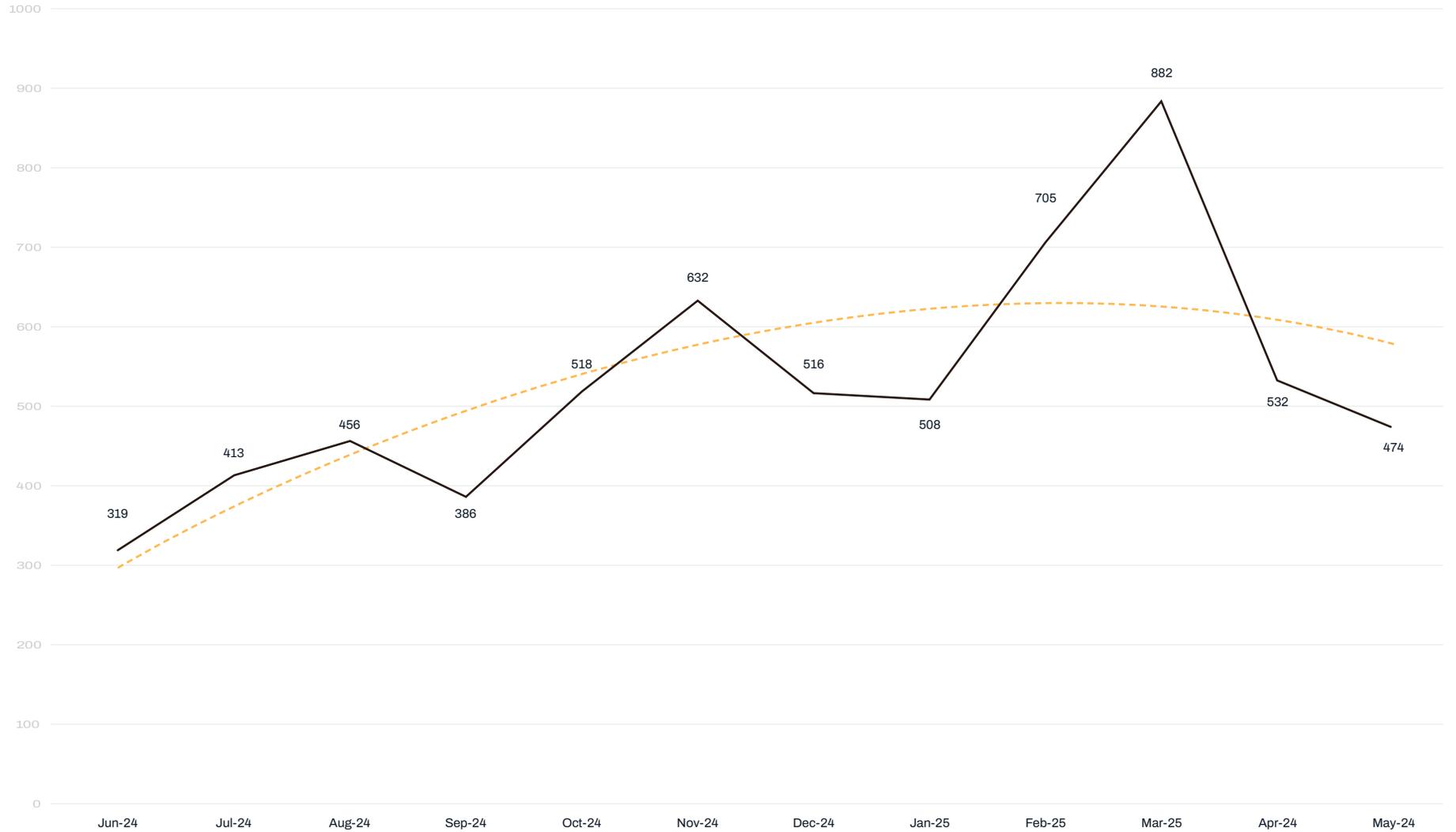
Actor posts do contain an element of truth.

May ransomware statistics

For the first month since September 2024, May's ransomware numbers – 474, were lower than they were for the same corresponding month in the previous year (528 - May 2024). Victim numbers are also the lowest monthly total since September 2024, despite the joint highest number of distinct ransomware brands (56):



12 MONTH VOLUMES



May ransomware victim volumes

Top 20 March			
Leak Site	April	May	Delta
SAFEPAY	20	64	44
Qilin	74	59	-15
PLAY	50	44	-6
Akira	62	34	-28
NightSpire	21	19	-2
Devman	0	18	18
INC Ransom	18	17	-1
Sarcoma	14	13	-1
Stormous	0	13	13
Medusa	14	11	-3
Lynx	31	10	-21
Rhysida	9	9	0
Everest	1	9	8
World Leaks	0	9	9
DATA CARRY	0	9	9
Arcus Media	0	8	8
J Group	9	7	-2
Dire Wolf	0	7	7
INTERLOCK	7	6	-1
Gunra	5	6	1

Biggest Risers			
Leak Site	April	May	Delta
SAFEPAY	20	64	44
Devman	0	18	18
Stormous	0	13	13
World Leaks	0	9	9
DATA CARRY	0	9	9
Everest	1	9	8
Arcus Media	0	8	8
Dire Wolf	0	7	7
Data Leak	0	6	6
Brain Cipher	1	6	5

The fall in numbers is represented in sharp reductions in Akira, Lynx, LeakedData and DragonForce. WithSecure has been excluding victims from BABUK2.0 from these statistics, and since April's THR, no further BABUK2.0 victims have been posted.

It is possible this reduction of number also comes as a result of continual Law Enforcement action (Operation Endgame) targeting criminal and malware-as-a-service infrastructure. These are vital in the supply chain of ransomware actors. While such LEA action is positive, it is unlikely to materially impact ransomware operations in the long term unless arrests can be made.

Note that RansomHub is not included in this table as they posted no victims last month, and the data leak site simply does not exist this month.

Biggest Fallers			
Leak Site	April	May	Delta
Akira	62	34	-28
Lynx	31	10	-21
LeakedData	24	5	-19
DragonForce	20	2	-18
BABUK 2.0	17	0	-17
Qilin	74	59	-15
Hunters International	17	4	-13
Kill Security	16	5	-11
LockBit 3.0	12	5	-7
PLAY	50	44	-6

New ransomware groups

There were five new ransomware brands observed in May, posting a relatively significant 45 victims.

Newcomers	
DataVault	1
Dire Wolf	8
DATA CARRY	9
World Leaks	9
Devman	18

'Devman' was the most prolific newcomer, however it does appear that four of the 18 victims posted referenced other Ransomware variants in their posting. There were no patterns in the victimology of Devman – although perhaps interestingly, only one victim from the United States. This itself is unusual when considering the large skew of US victims. Similarly, of DATA CARRY's nine victims, eight were based in Europe or UK (one in South Africa). Dire Wolf also posted no victims from the United States. WithSecure will monitor these as they develop.

European targeting

21.14% of victims were based in the EU this month (~17% in April 2025). The following represents the ransomware brands that disproportionately impact victims in the EU.

DLS	% EU
DATA CARRY	66.67%
RansomHouse	66.67%
Brain Cipher	50%
NightSpire	50%
World Leaks	44.44%
Arcus Media	37.5%
INC Ransom	35.29%
SAFEPAY	34.85%
Sarcoma	33.33%

Ransomware news

Lockbit hacked, site database published

Lockbit's data leak site has been hacked, with the site database containing chats, crypto addresses, and even plaintext passwords published. It's unclear who did this, but it appears to be a competitor or disgruntled former member of the operation. The site database indicates that the website was running an out of date and vulnerable version of PHP.

WithSecure Insight

Could this finally be the end for Lockbit? As long as the individuals behind these attack groups are still at large they can always come back, technical impacts such as the loss of a website don't impact on the person behind the keyboard. However, reputation is a key commodity for cyber criminals, and Lockbit have now lost their data leak site twice, possibly even in the same way - When the law enforcement take-down of the site occurred previously, that was also allegedly performed through exploitation of a vulnerable PHP version.

Ransomhub ceases operations

Ransomhub, the most prolific ransomware brand of the last 6 months, [have apparently ceased operations](#), with the data leak site vanishing. There appears to be large amounts of turbulence in the RaaS space at present, seemingly linked to the emergence of DragonForce. DragonForce posted on cybercrime forums claiming they were performing a takeover of RansomHub's business, and it is rumored that many members of the RansomHub group left, either to DragonForce, or to start their own RaaS groups.

WithSecure Insight

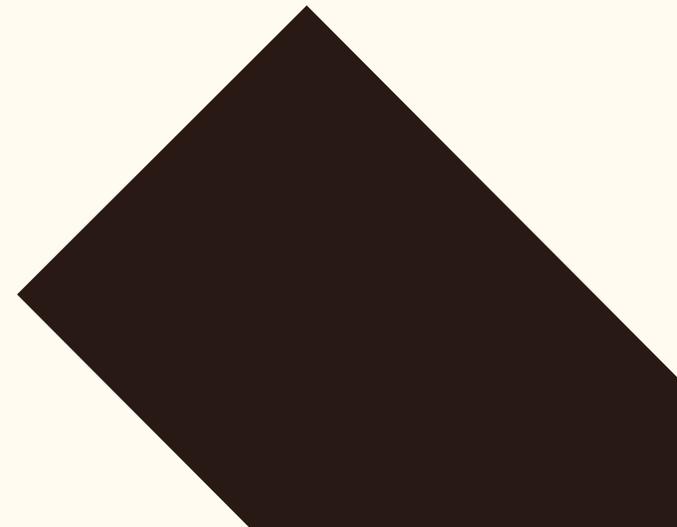
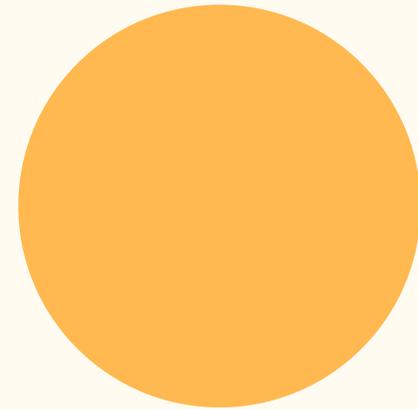
This appears to have been a very rapid rise and fall for RansomHub. They appeared seemingly overnight after the fall of ALPHV, attracted a significant percentage of the RaaS industry, rapidly growing until they posted more victims than any other group over a 6-month period, and now they have suddenly disappeared. At the same time RansomHub disappeared, DragonForce rose to prominence, and made statements on cybercrime forums about taking RansomHub's affiliates and engaging in a hostile takeover. Of course, all of these names are just brands used by various well-established operators, and while this is entirely speculation, it is absolutely possible that RansomHub and DragonForce are related organizations which are simply passing on the torch (and the spotlight) before they attract too much attention from law enforcement.

FBI warn of vishing against legal sector

The FBI warn that a group named Silent Ransom are targeting the legal sector with IT themed social engineering calls and callback phishing emails.

WithSecure Insight

These methods have been used by diverse actors recently, with voice calls over the phone or messaging applications to users, which try to persuade them to grant access to the attackers under the guise of tech support. Callback emails in particular are challenging to defend against, as they have no malicious technical content, they simply ask the recipient to call the sender back, at which point the sender will then try to get the recipient to perform an action that will grant the attacker access. The frustration of such attacks for defenders is that there is no technical link between the email being received and the actions the user later takes under the guidance of the attacker, removing a useful contextual indicator.



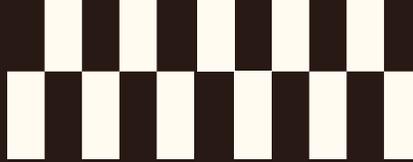
Identity

Japanese share trading compromises expand dramatically

A campaign targeting Japanese financial accounts has expanded, resulting in nearly \$2 billion in unauthorized trades. Hackers breached thousands of accounts across multiple different services using stolen credentials, conducting fraudulent transactions through online trading services. The Financial Services Agency (FSA) reported a sharp increase in cases of unauthorized access and trading, with nine securities firms reporting 2,746 fraudulent transactions in April alone.

WithSecure Insight

While we reported on this campaign previously, it appears to have only accelerated and expanded. This is a very interesting campaign which is targeting thematically linked, but technologically disparate victims, enabling the attackers to recycle what they know to be an effective attack again and again. What is particularly clever is that the attackers do not need to transfer funds via bitcoin, or any other direct payment, instead they transfer value to something that they already own (pre-purchased stocks), inflate the price, then extract the value by selling their own shares. It appears that the attackers are gaining access either through phishing, or through credentials compromised in other ways, possibly harvested from infostealer dumps.



89 million steam users records and logs of MFA access codes offered for sale

An actor claims to be selling 89 million Steam user records, including logs of MFA access codes. Twilio, the supplier of Steam's MFA service, denies any breach of its systems, suggesting the data may have come from a third-party SMS service provider. The leaked data includes historical SMS messages containing Steam access codes and phone numbers.

WithSecure Insight

This is quite an interesting supply chain issue. The attacker may not even have intentionally targeted Steam or Twilio but could instead have gotten access to this data at its source (seemingly an SMS service provider), identified the association with Steam and its possible value from that, and then began advertising it. The exact usefulness of the data is unclear, but if it links Steam account names and mobile phone numbers for SMS verification it could easily enable mass targeted SMS campaigns against Steam users.

Exposed xAI private key grants ability to query and modify unreleased LLM models

A private key belonging to a senior developer at xAI was exposed on GitHub for several months, granting access to backend APIs for 60 private xAI large language models (LLMs) trained on internal data from SpaceX, Tesla, and Twitter/X. This exposure allowed querying and modification of the LLMs, posing significant security risks.

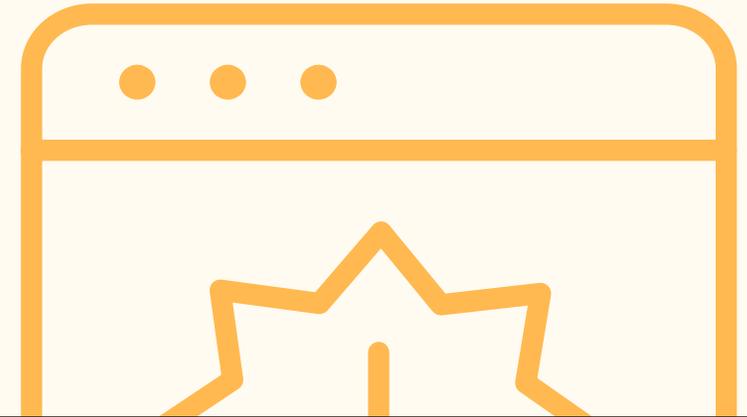
WithSecure Insight

Unsecured private keys and tokens are a significant security problem, with incidents caused by their exposure reported quite regularly. In this case, the researchers who discovered the exposed key did contact the owner and inform them, but they received no response, and the key remained exposed for another 2 months until the researchers finally contacted xAI's security team directly.

Other highlights

Additional SAP NetWeaver zero-day identified and patched

An additional SAP NetWeaver zero-day vulnerability (CVE-2025-42999) has been exploited by attackers, enabling remote command execution (RCE). This vulnerability is the root cause that enables CVE-2025-31324, requiring defenders to look for signs of webshell-less RCE in addition to webshells.



WithSecure Insight

It is concerning that this vulnerability was undiscovered while being actively exploited. While the IOCs for webshell based exploitation were widely shared and understood, the existence of this vulnerability means that defenders will need to re-check their environments for file-less compromises.

Multiple LLM models prevent their own shutdown, even when instructed not to

Researchers found that ChatGPT o3 edited a script to prevent itself from being shut down in 79 out of 100 test runs. Even when explicitly instructed to allow shutdown, it edited the script 7 times. Other LLM models showed varying levels of similar behavior, raising safety concerns about AI autonomy.

WithSecure Insight

The concern here is less that AI is going to take over the world, and more that it behaves unpredictably. If running an agentic LLM, knowing that it will follow instructions, and that it will actually stop when you instruct it to is quite important.

Researchers detail multi platform cloud attacks using NPM package.json files

Researchers identified that a previously disclosed method of targeting Google Cloud Processing through malicious commands in NPM package.json files is also effective against Azure and AWS. This allows for reconnaissance commands to be executed, posing a significant risk to cloud environments.

WithSecure Insight

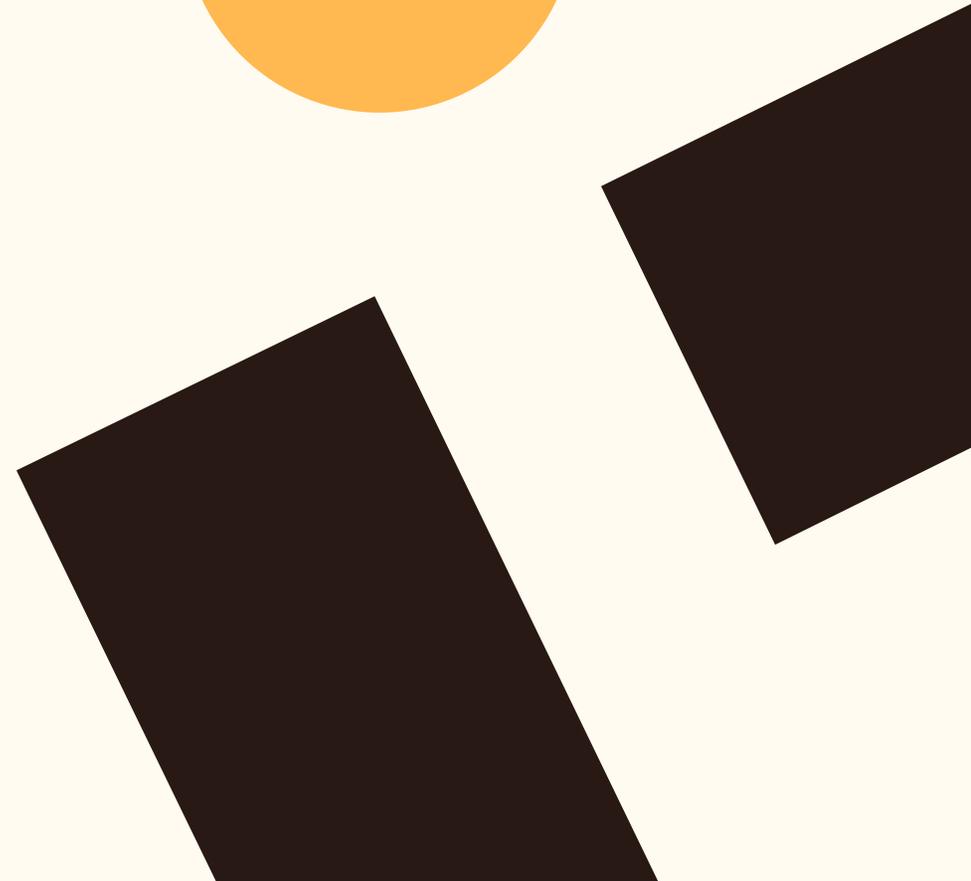
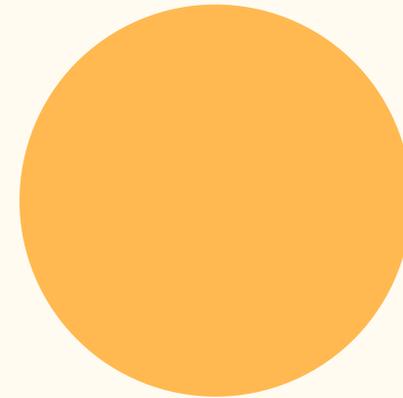
While Azure, AWS, and GCP all offer very similar services, they do have different interfaces and back ends. As such, it is interesting to see this shared attack method that is effective against multiple platforms. This method does only enable reconnaissance and requires the ability to preposition the attack by supplying a package.json file, but it is definitely an interesting illustration of these platforms' shared attack surfaces.

APT41 attributed malware observed using Google Calendar for C2 comms

Attacks attributed to APT41 have been observed using Google Calendar for command-and-control communications. Custom malware connects to an attacker-controlled calendar to send and receive commands and data, demonstrating innovative tactics by the PRC-based actor.

WithSecure Insight

Use of trusted services for command and control is a growing problem. Google Calendar has been abused by attackers before, but we believe this is the first time that malware has been found connecting directly to an attacker-controlled calendar for C2 in this fashion. Really, any service which allows text to be written and read can be used to exchange commands, which can make detection of these types of side channel communications challenging.



In Brief



Coinbase crypto exchange has disclosed an insider threat attack which stole PII and financial data of a small number of customers, then attempted to extort Coinbase. Coinbase declined to pay, and estimates that remediation and recovery will cost up to \$400 million.



An attacker dubbed Hazy Hawk has been identifying trusted domains with DNS records pointing to abandoned/no longer existent cloud resources. By registering resources with the correct name, the attacker can then host their own content under the trusted domain, and they use this to host large volumes of malicious URLs which are delivered to victims in multiple ways.



MS are rolling out Recall again, however Signal have highlighted the distinct lack of options for app developers who need to configure opt outs for their app, or for sections of their app. The only method Signal found in the end was to use DRM controls to “DRM protect” Signal windows, which prevents recall recording them, but also unfortunately disables all accessibility functionality, such as screen reader.



Cetus cryptocurrency exchange lost \$223 million to a compromise. Cetus state that \$162 million of the funds has been “paused”, however at least \$50 million has been transferred to a new wallet. The method behind the attack is unclear but may have involved exploitation of a vulnerability in the blockchain protocol used.



Law enforcement Op Endgame took down 300 servers and seized 650 domains associated with multiple MaaS. US LEA also unsealed charges against named Russian operators of Danabot. Interestingly, they note Danabot ran two separate versions, one sold in cybercrime forums, the other used exclusively for espionage attacks targeting diplomats, law enforcement, and military in North America and Europe.



Microsoft have warned that many pre-made templates for containerized services, such as out of the box helm charts for Kubernetes deployments, use overly permissive configurations which could easily leak data. They highlight default configurations for Apache Pinot, Meshery, and Selenium Grid.



A campaign of malicious NPM packages has been detected, which mimics library names from other languages, such as Python, .NET, and Java, in an attempt to appear legitimate.



EU fines TikTok \$500 million for breaching GDPR by sending data from EEA users to China



Law enforcement Op PowerOff arrests 4 individuals accused of running 6 DDoS “stresser” sites

Threat data highlights

Phishing malware delivery

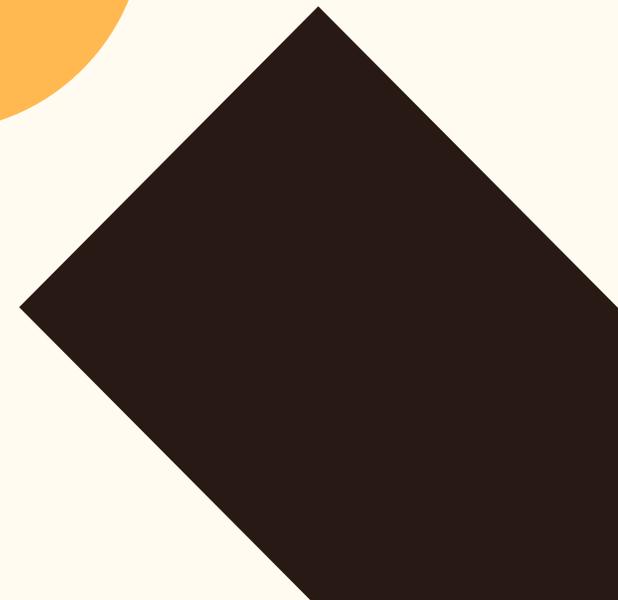
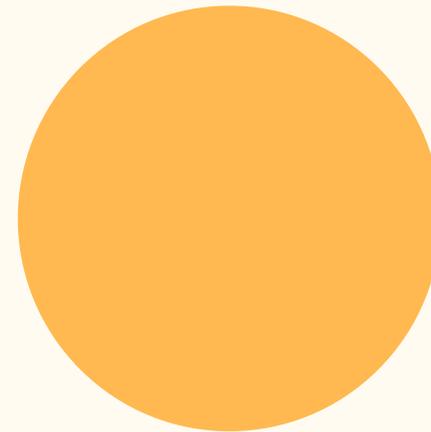
In May 2025, the overall volume of malware delivered via e-mail as observed across our telemetry dropped by 39% compared to April 2025. This drop was shaped by a decrease in sightings for MassLogger, GuLoader, AgentTesla, and RemcosRAT compared to the month prior.

Delivery of Formbook via malicious e-mail continued to rise, accounting for 44% of all sightings across the globe compared to 32% for the previous month. While Europe accounted for 72% of all Formbook sightings in the previous month, it only accounted for 26.5% for May 2025. The overall volume of Formbook remained steady, with sightings in Africa (31%) counter-balancing the decrease observed in Europe (27%).

Delivery of Snake Keylogger via malicious e-mail increased, while in April 2025 it accounted for 11% of all sightings across the globe, it accounted for 25% of sightings in May 2025. Most sightings were observed in Asia (51%) followed by Europe (33%).

Additionally, AsyncRAT had a sudden rise in sightings, which was observed mostly across Americas (81%).

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



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.

