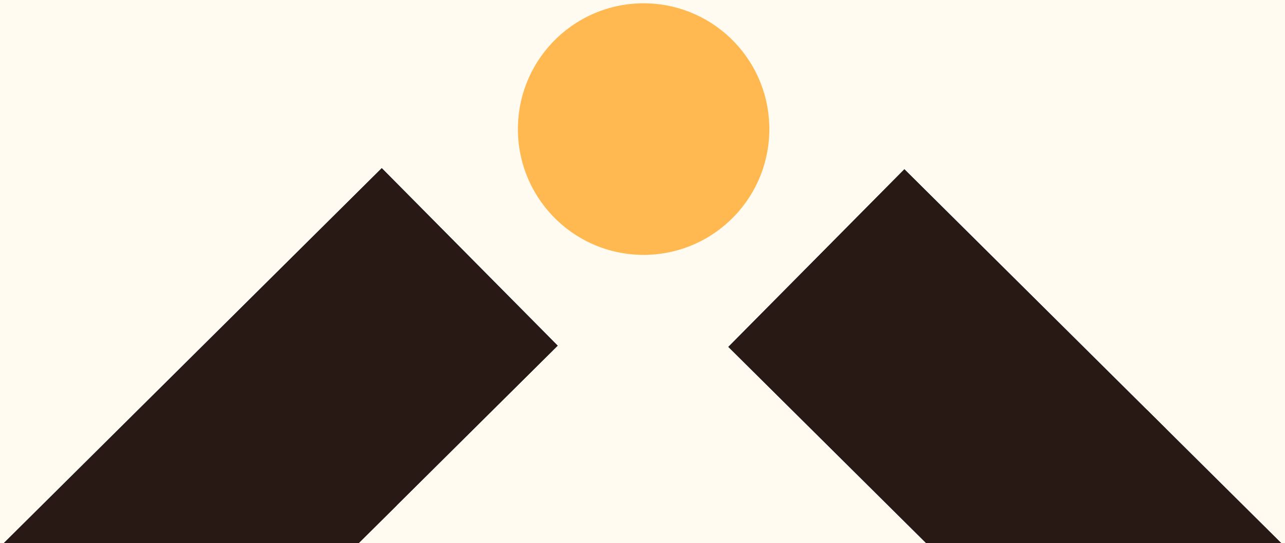
WITH secure

Threat Highlight Report

June 2025

Table of Contents



Foreword

“Scattered Spider continued to make waves this month as their sectoral targeting and rapid-fire attacks moved to focus on the US Insurance sector. Something that is likely to be a bit more impactful for many in the industry, however, is the disclosure of a Citrix NetScaler vulnerability that has been dubbed CitrixBleed2. Much like its namesake, this vulnerability allows remote attackers to read the memory of NetScaler devices, extracting credentials and secrets at their leisure. Oh dear.

The ransomware industry continues to be turbulent and changeable, which is typically good news for defenders. Indeed, this is the third month in a row that ransomware victim numbers have fallen, the first time this has ever happened since we began tracking them in January 2022.

We have sections on Identity, CNI, Cloud, and AI this month, with interesting and important stories on threats, risks, and cybersecurity developments in each category.

As ever we intend on recording a podcast this month, where we will discuss these stories in more detail, so please do listen via your preferred podcast store front for additional insights.”

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

Monthly highlights

Scattered Spider campaigns continue against new sectors

In May it became known that Scattered Spider attackers had targeted the UK retail sector with social engineering-based ransomware attacks. It is reported that the actors have now pivoted to US insurance companies. Mandiant reports that multiple attacks on US-based insurance companies share common tactics, techniques, and procedures (TTPs) associated with Scattered Spider. At this time five US insurance companies, including Aflac, Erie Insurance, Tokio Marine North America, and Tokio-owned companies Philadelphia Insurance Companies and First Insurance Company of Hawaii, have disclosed breaches believed to be part of Scattered Spider's campaign targeting the insurance sector. Aflac described their compromise as part of a sophisticated cybercrime campaign against the insurance industry, involving data theft and system disruption.

Tata Consultancy Services (TCS), which some reports suggested were linked to the UK Retail attacks, have stated on their Q2 results call that none of their systems or users were compromised in the cyberattacks on UK retailers Marks and Spencer (M&S) and Co-Op.

However, it is worth noting that if the attacks targeted M&S and Co-Op user accounts and systems by socially engineering technical helpdesk services managed by TCS, the statement could still be true. This highlights the possible complexity of attributing responsibility in cyber incidents involving third-party vendors.

The UK insurance industry's Cyber Monitoring Centre has publicly assessed the compromise of UK retailers Marks and Spencer and Co-Op as a single combined cyber event, with a probable financial impact of up to £440 million. This assessment is significant as while there have been suspicions that this was the case, this is the first public assessment that has been made which links these attacks.

WithSecure Insight

Scattered Spider are an interesting group because they are a loosely identified group of operators with shared characteristics and TTPs, not a brand in the way that ransomware groups are. They are typically not high volume, but they seek out headlines and notoriety through their attacks, as well as financial reward. While it is interesting to see their pivot from retail to insurance, there is very little that relates the two industries, and Scattered Spider's inherently chaotic nature means it is difficult to predict how long their focus will stay on the US insurance industry, or what sector they will move to next.

CitrixBleed2?

CVE-2024-5777, a memory overread vulnerability affecting Citrix NetScaler, has been exploited in the wild. This vulnerability, similar to CitrixBleed, is one of three related issues, including a memory overwrite vulnerability (CVE-2025-6543) and an improper access control vulnerability (CVE-2025-5349). Initially, Citrix stated that these vulnerabilities were only exploitable via the management interface, but later updates revealed they could be exploited from any interface if the NetScaler was configured as a VPN gateway, ICA Proxy, CVPN, RDP Proxy, or AAA virtual server, significantly increasing the exploitation scope.

WithSecure Insight

This vulnerability is so similar to CitrixBleed that it really is well suited to the name CitrixBleed2. That similarity also means that there is a chance of similar levels of abuse and disruption due to its exploitation. Strictly speaking, the memory overwrite vulnerability is more severe as it allows remote code execution, however, the nature of NetScalers means that being able to simply extract the credentials and come back later with valid credentials is both more practical and easier to exploit at scale.

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 number of paying victims greatly increases, 'total' ransomware numbers may also appear to decrease.

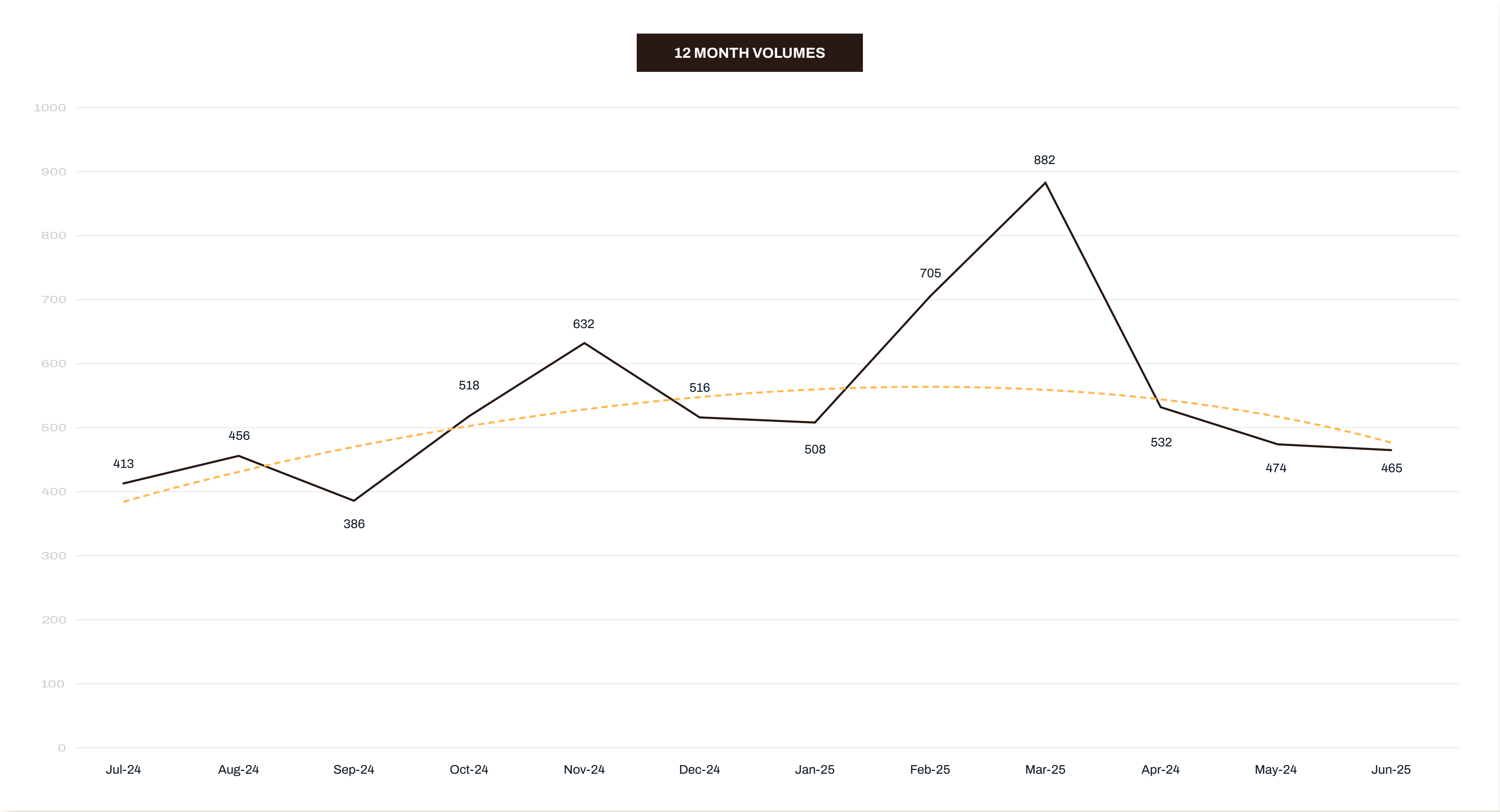
With this said, we can draw some insight from this data with sensible assumptions – and recognizing the data isn't perfect, it does provide a decent gauge on the ransomware landscape.

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.

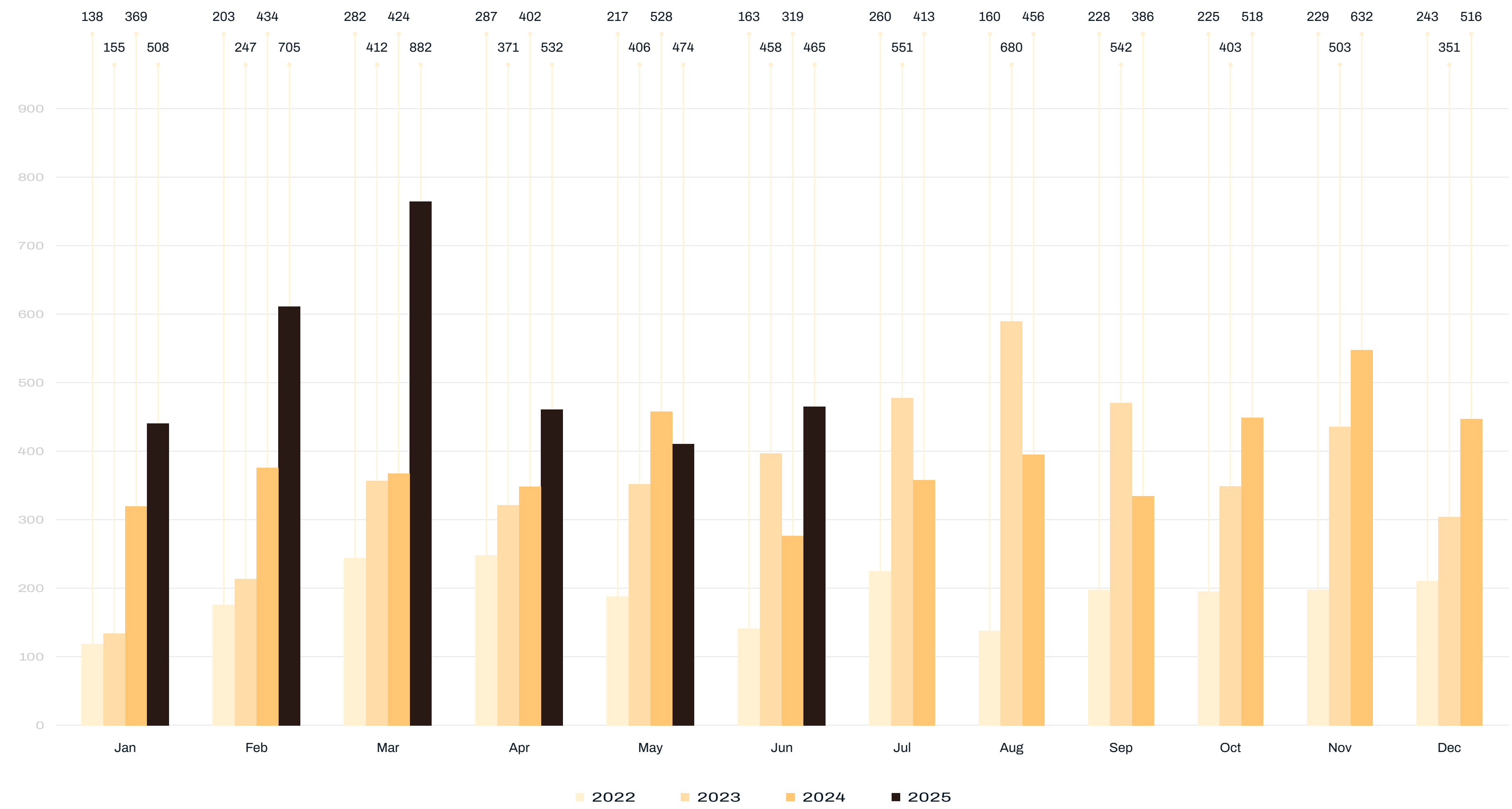
June ransomware statistics

In 2024, June's ransomware leak site numbers were lower than previous months. This is also the case for June 2025. Numbers dropped moderately to 465 from 474, with 5 fewer distinct ransomware brands being observed.

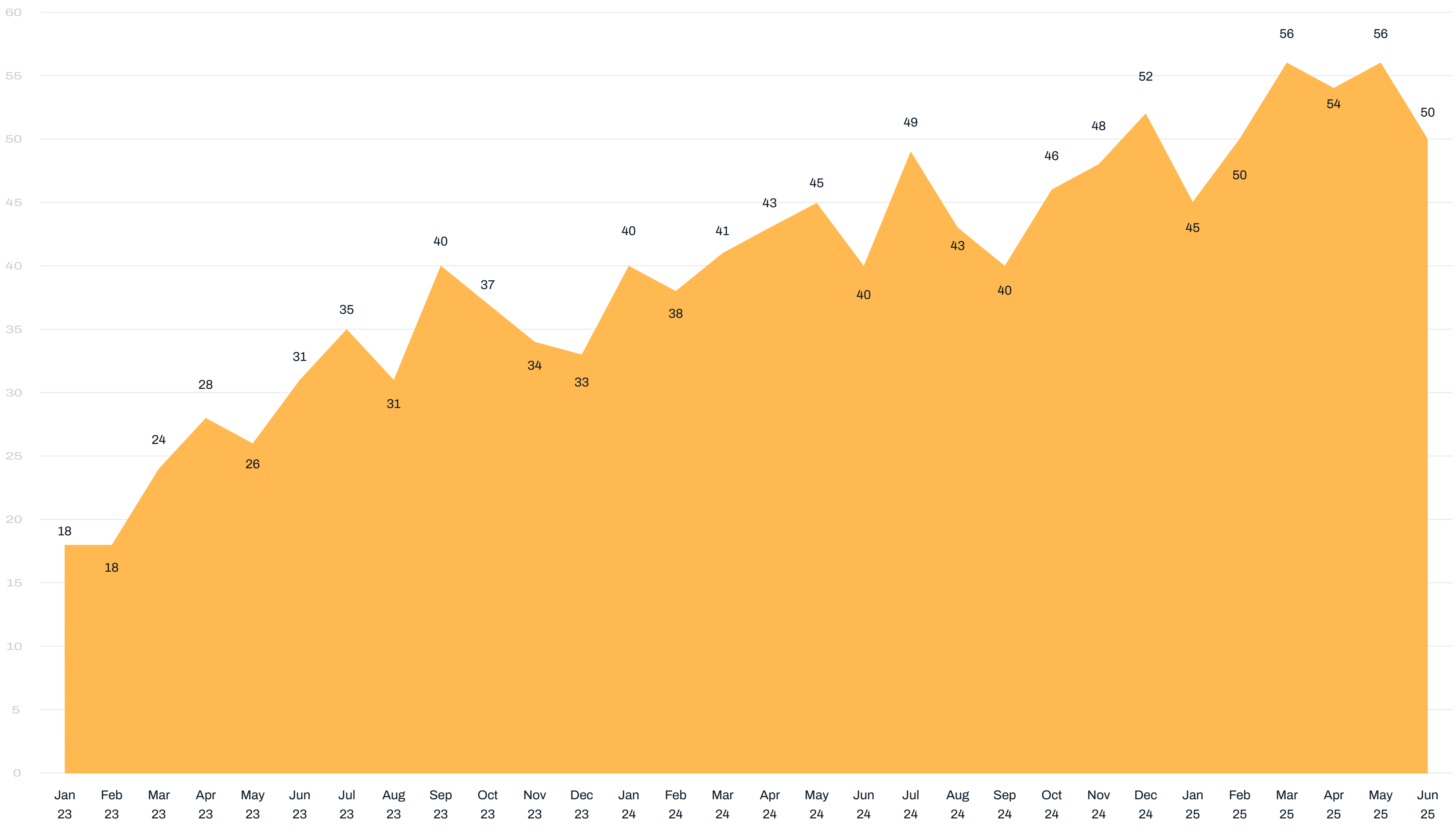


This also marks the third month in a row where victim numbers have dropped – something that has not happened since recording started from January 2022.

Ransomware year-on-year



RaaS brands observed (Unique)



June ransomware victim volumes

Qilin and DragonForce have shown significant increases, and also two new data leak sites have made it into the top 5 this month, Warlock and Global. As ever, a new data leak site, or a new brand name, most likely does not indicate new actors or operators, but instead a rebrand or re-organization within the existing industry.

Biggest Risers			
Leak Site	**May**	**June**	**Delta**
Qilin	60	91	31
DragonForce	2	25	23
Warlock	-	19	19
Global	-	16	16
World Leaks	9	22	13
INC Ransom	17	26	9
Lynx	11	20	9
TeamXXX	-	8	8
INTERLOCK	6	13	7
Kraken	1	8	7
Kawa4096	-	6	6

A dropping off in numbers posted by Safepay (-37), Devman (-17), Play (-15) and Nightspire (-10) are, in the main, balanced by gains in Qilin (+31), DragonForce (23) and newcomer Warlock (+19).

WithSecure expects that the continual decline of victim numbers posted to ransomware victim blogs comes as a result of continual law enforcement agency (LEA) action (such as Operation Endgame) targeting criminal and malware-as-a-service infrastructure, though we must recognize that in the long run statistics will be influenced by increased availability of cyber insurance. The criminal services being targeted by law enforcement are vital in the supply chain of ransomware actors. While such LEA action is positive, WithSecure still expects ransomware operations and victim volumes to recover in the long term.

Biggest Fallers

Leak Site	May	June	Delta
Safepay	64	27	-37
Devman	18	1	-17
Play	44	29	-15
NightSpire	19	9	-10
Sarcoma	14	6	-8
Stormous	13	5	-8
DATACARRY	9	2	-7
Arcus Media	8	2	-6
Brain Cipher	6	0	-6
Rhysida	9	4	-5
Hunters International	5	0	-5

New ransomware groups

As in May 2025, there were five newcomers in June 2025, posting a significant 50 victims.

Biggest Fallers	
WALocker	1
Kawa4096	6
TeamXXX	8
Global	16
Warlock	19

Warlock has an interesting victim set. No victims posted are based in the United States – highly unusual for a ransomware collective. Furthermore, there appears to be victims reposted from previous, now defunct ransomware sites. This is not uncommon if there is either an overlap in affiliate who did not manage to secure a ransom from the victim, or if a new ransomware brand is seeking to attain a level of legitimacy through populating their site.

Global's victims have a much more 'typical' global distribution. Five of the 16 victims posted are involved in the medical sector, and all but two are very small businesses.

European targeting

As in May 2025, there were five newcomers in June 2025, posting a significant 50 victims.

DLS	% EU
Kraken	50
Sarcoma	42.86
Hellcat	33.33
Akira	27.91
NightSpire	27.27
Warlock	26.32
TeamXXX	25
Global	18.75
Qilin	18.18
RALord	18.18
Baseline	15.18

Ransomware news

Fog ransomware attack uses novel tools and TTPs

A Fog ransomware attack on a financial organization in Asia involved the deployment and use of unusual tools, including the legitimate Syteca (formally Ekran) employee monitoring tool and the GC2 “pen test” tool, which utilizes Google and Microsoft online services for command and control (C2) and data exfiltration. Interestingly, the attacker was observed attempting to maintain persistence even after the ransomware payload was detonated.

WithSecure Insight

It is very interesting to see a ransomware attack abusing a rare tool, instead of the common LoLbins. Syteca has been abused in the past in an attack by a probable Chinese state sponsored actor, and its abuse makes sense, as it provides a road range of surveillance capabilities which can easily be abused by attackers. While it would be a stretch to suggest that this activity could be linked to that of an actor who used the same tool in a single incident multiple years ago, the fact that the attacker attempted to maintain persistence after deploying ransomware does raise questions. This could indicate that ransomware detonation was intended as a distraction, or to hide forensic indicators from the initial access phase.

BlackBasta TTPs cross-pollinate to multiple other groups

BlackBasta's tactics, techniques, and procedures (TTPs) of using Teams vishing to deliver Python payloads have been adopted by other groups, including BlackSuit, BlackLock, and CACTUS. BlackSuit is now using an updated version of BlackBasta-associated malware that employs OneDrive, Google Sheets, and Google Drive for C2.

WithSecure Insight

TTPs are always cross pollinating across the ransomware industry as groups form, merge, and split up again, and as operators move around. This particular combined TTP of Python payloads via Teams phishing is quite specifically BlackBasta however, so tracking its uptake across the industry gives the opportunity to see how turbulent the industry is right now, and much disturbance there has been. Unfortunately for defenders, Teams phishing has shown to be quite effective, as it abuses employees' habits and expectation that messages sent via Teams are internal, and inherently more trustworthy than an email or SMS.

Individuals behind Conti and Trickbot doxxed

An actor is doxing members of the Conti and Trickbot groups, publishing internal information such as identities, chat logs, ransom negotiations, and video recordings. German authorities have corroborated the accuracy of at least one of the identifications made. The actor claims to be an independent investigator but is suspected to be a disgruntled group member or competitor.

WithSecure Insight

The nature of the actor who is distributing this information is unclear. This could be part of a law enforcement operation, an internal cybercrime industry spat, or a disgruntled former employee/partner. Whatever the cause, it is good to see cybercriminals being shown that they are not untouchable. Historically of course, even if individuals have not performed cyber crimes in jurisdictions where they live or can be extradited to, they are often found to have performed significant tax evasion, which presents its own special set of problems.

UK NHS confirms Qilin ransomware attack killed at least one patient

A Qilin ransomware attack on the NHS, which affected multiple London hospitals, has been confirmed to have directly led to the death of at least one patient. The attack targeted Synnovis, a pathology services provider, causing widespread disruption to diagnostic services and delaying blood test results. This incident highlights the severe impact of cyberattacks on healthcare services and patient safety.

WithSecure Insight

Sadly, this is exactly what is expected when cyber attackers target healthcare, and the threat of such absolute harm that comes from disrupted services is exactly why attackers will happily target healthcare.

Identity

Google account phone numbers can be brute forced

A researcher has discovered a method to identify the phone number linked to a Google account by combining a legacy password reset form with no brute-force protection and a behaviour exhibited by Google Looker Studio which allowed any google user to find the display name of any other Google user. This vulnerability opens the victim to further targeting, including SIM swapping attacks.

WithSecure Insight

Being able to derive the phone number linked to an account opens up the victim to SIM swapping and multi-medium phishing attacks and social engineering. What is maybe most concerning about this however is the illustration it provides of the sprawling nature of Google's Internet-facing services. It is likely that the continued existence and accessibility of the legacy authentication portal was completely unknown to Google. While the specific behavior of Google Looker Studio was probably known to those who implemented and maintained it, the wider impact of that display name lookup functionality on the rest of the Google ecosystem was almost certainly not known. Complexity is the enemy of security, and complex cloud services are, by definition, complex.

North Face discloses data breach via stolen credentials

North Face has disclosed a data breach, making it the fifth fashion brand to report a breach in recent months. North Face attributed the breach to credential stuffing due to credential reuse by customers. However, it is unclear whether the breach was solely due to credential reuse or if attackers harvested North Face customer credentials from infostealer dumps.

WithSecure Insight

It is difficult to reliably determine whether an attack was performed through credential stuffing due to credential re-use, or through credentials stolen by infostealers. A possible differentiator might be if logs showed that large numbers of non-existent credentials were attempted alongside the successful logins. However, multiple compromises in this sector in a short time is interesting, especially as they seem to be targeting customer credentials. In this case, North Face reported that the impact was the theft of PII from within the customer accounts, which suggests that no purchases were able to be made through the accounts. That could be because the attackers were not able to, or because North Face identified the attack and declined all associated purchases.

Russian APT phishing campaign targets App Specific Passwords (ASP)

A Russian state-sponsored threat actor, attributed with low confidence as APT29, has been targeting prominent academics and critics of Russia in a phishing campaign active since at least April 2025. The attackers attempt to get victims to create and send an application-specific password (ASP) for their Google account, granting persistent access to the victim's Google mailbox.

WithSecure Insight

ASPs are a legacy feature allowing applications that do not support modern authentication methods to be linked to the user's Google account, essentially authenticating them to access the account with permissions granted by the user. There have also recently been campaigns by Russian actors which abused device codes, which provide very similar functionality to physical devices. These kinds of legacy protocols allow attackers to completely bypass modern authentication methods. Though these attacks do require social engineering to convince the user to grant access, the legacy nature of the functionality often means that users are not familiar with the implications of the actions they are asked to perform.

M365 to begin blocking insecure, legacy authentication protocols

A new security update for Microsoft 365 will block browser authentication to SharePoint and OneDrive using the Relying Party Suite (RPS) and FrontPage Remote Procedure Call (FPRPC) protocols. These legacy protocols are vulnerable to brute-force and phishing attacks and do not support multifactor authentication, making them highly insecure.

WithSecure Insight

Much like the previous story, these are yet more legacy authentication protocols. The FPRPC protocol is from Microsoft FrontPage the last release of which was in 2007. The existence and usability of these protocols makes modern authentication and MFA optional, which allows attackers to completely bypass them. If these two protocols are being blocked, it does raise the question of whatever legacy/insecure protocols are supported by M365, and is there any way to block their use within a tenant?

CNI

Norwegian dam flow rate controlled by unknown attackers

Unknown attackers took control of a dam in Risevatnet, Norway, for several hours through an internet-exposed web control panel with a weak password. The attackers maximised the dam's flow output during this time.

WithSecure Insight

While physical damage is difficult to achieve through such control panels, this incident highlights the potential risks. Indeed, while physical damage to the system might be difficult, when considering the worsening drought conditions in central Europe at present, it's entirely possible that simply letting water flow out of a damn could have severe real-world impact.

Empty shelves in Russia due to cyber-attack

The Russian Federal State Information System for Veterinary Surveillance was taken offline due to a cyber-attack, disrupting the supply of animal products like meat, eggs, and milk. This system is critical for certifying the origin and handling chain of animal products under Russian law. The attack has led to empty shelves in shops, demonstrating the significant impact on daily life and the potential vulnerability of similar systems in other countries.

WithSecure Insight

Critical national infrastructure makes people think of energy grids, train networks, and maybe financial systems. However, there are a multitude of boring, taken for granted, yet highly essential systems that are needed for modern civilization to function. The Russian animal products origin system that was taken down is essentially just a database for tracking a product back to its point of production, but without it, logistics chains grind to a halt. Similar systems will exist in most countries, and their disruption could have similar very visible and affecting impacts on individuals, and on social stability. CNI is incredibly broad, and it may well be that only when a system is taken down will we understand just how much we relied on it.

Cloud

Multiple vulnerabilities and misconfigurations identified in Salesforce

A researcher has identified 5 vulnerabilities and 20 configuration-related risks in Salesforce, which have now been patched. These issues include unenforced access control checks, data-leaking caching mechanisms, readable API keys within components, and insecure default permissions. While patches have been issued, 16 of the configuration risks are the responsibility of customers to address.

WithSecure Insight

It's great to see this kind of research taking place, and so many vulnerabilities being addressed. However, it is worrying that so many vulnerabilities existed. More worrying, is that many of the configuration-related risks remain, and can only be fixed by individual customers/tenants modifying their configuration to align with updated best practices. If people regularly reviewed best practices and implemented them promptly within their environments, cybersecurity would be a much smaller industry, both on the attacker and defender sides.

Scattered Spider-esque attackers target Salesforce instances

Google Threat Intelligence Group (TIG) reports that a ScatteredSpider (UNC3944) adjacent group, UNC6040, is targeting Salesforce users with voice-phishing campaigns. The attackers convince users to add a modified Salesforce Data Loader app to their instance, allowing data exfiltration and lateral movement within the system.

WithSecure Insight

Scattered Spider is an extremely loose terminology and threat grouping, describing as it does more a culture, set of TTPs, and preferred communications network, so describing an actor as Scattered Spider adjacent tells us the actor behaves in a certain way, but is not believed to be the specific actors to whom the other current Scattered Spider activities are attributed.

The targeting of Salesforce with a Salesforce app is interesting – This methodology is quite similar to that which has been used in Scattered Spider attributed attacks to target Identity as a Service in the past – A social engineering approach which takes advantage of a lack of understanding of a complex cloud service provided by a third party. Simply by being familiar with the Salesforce control panel and the way that Salesforce apps can be used, the attacker is better informed than most users of Salesforce that they might interact with.

Cisco ISE cloud deployments suffer provider specific hardcoded credentials

Cisco has patched a critical 9.9 severity vulnerability (CVE-2025-20286) in Identity Services Engine (ISE). The vulnerability stems from all ISE cloud deployments of the same release version on the same cloud provider (AWS, Azure, and OCI specifically) having identical credentials, posing a significant security risk.

WithSecure Insight

It is very unusual to see a vulnerability that specifically affects cloud deployments of software. In this case, it appears that some characteristic of the standard cloud environment was being used during installation to generate a key, token, or password, and due to the standardized nature of cloud environments within each provider, that key was also being unintentionally standardized. This is not a good situation to be in for users of this software, as that key is then available to anybody with access to an installation on that cloud.

AI

New attack bypasses tokenization based LLM protections

A new attack against large language models (LLMs), named TokenBreak, exploits the discrepancy between how the LLM and its tokenizer interpret prompts. By inserting specific characters, attackers can cause the tokenizer to split the text in a way that the LLM still recognises the prohibited input, bypassing the intended restrictions.

WithSecure Insight

This attack works because the tokenizer is essentially not as intelligent as the LLM it is attempting to protect. As such, a prompt can be obfuscated in such a way that it is not understood by the tokenizer, but it is understood by the LLM.

Remote prompt injection via email vulnerability patched in M365 Copilot

An attack named EchoLeak has been identified and patched in M365 CoPilot. This attack involves embedding a malicious prompt within a seemingly legitimate business email. When a user queries CoPilot with a business-related question, the malicious prompt is parsed, leading to unintended actions such as crafting a link that leaks sensitive internal data to an attacker's server.

WithSecure Insight

This kind of embedded malicious prompt is highly concerning in any environment where dynamic data is simply mass ingested into an LLM. The key to this attack is that the malicious prompt is hidden from the user, but present within the data which the LLM will be parsing when invoked by the user on their files and emails.

Other highlights

Trojanized SonicWall VPN client steals configuration on use

SonicWall has discovered that threat actors are modifying and redistributing a trojanized version of its NetExtender SSL VPN client. The trojan, delivered from a spoofed SonicWall website, steals VPN configuration and credentials when used to connect to a VPN, exfiltrating the data to an attacker-controlled server.

WithSecure Insight

This method of trojanizing a legitimate tool while keeping it functional was also observed in the KeeLoader campaign reported by WithSecure last month. This is a very effective method for attackers, as the downloaded tool performs as expected by the victim, giving no indication that it is malicious. Meanwhile, the malicious functionality is embedded into a sensitive process. In the case of KeeLoader, that was the password management process, while in this case it is accessing and authenticating to VPNs.

Malvertising inserts malicious text into benign pages

A malvertising campaign has been observed that exploits a feature of Google Ads to lead victims to legitimate sites containing malicious content. By pre-populating search bars with malicious messages, attackers can abuse legitimate websites to display their harmful content, such as fake phone numbers for support.

WithSecure Insight

This attack is very simplistic, but effective. Google Ad links display the destination domain, but not the whole URL. URL parameters can be used to pre-populate parts of a page, such as the search bar. In this way, a user may click on a Google Ad, and when the page loads see a message saying, “to resolve your issue please contact support on <phone number>”. However, that text is chosen by the attacker, and is not part of the benign page.

Critical vulnerability in IDE extension marketplace used by 8 million developers

A critical vulnerability in Open VSX, the open-source VS Code extension marketplace, has been patched. This vulnerability provided full control over the entire extensions marketplace, potentially allowing a malicious actor to push malicious updates to every extension on Open VSX. The flaw, which affected over 8 million developers, underscores the importance of securing software supply chains.

WithSecure Insight

Many people will have never heard of Open VSX before, but it acts as an extension marketplace for multiple opensource forks of Visual Studio Code which between them have millions of users. And of course, those users are developers, so the code they write may then be used by any number of further users. As such, compromising Open VSX and the developers who use it would provide access to even more downstream victims.

In Brief

CVE-2025-49113, a 9.9 severity flaw in RoundCube webmail has been identified and patched. This vulnerability has been present in the software for 10 years without being noticed, and (Seemingly) without being exploited.

International Law Enforcement Operation Endgame has taken down a syndicate which was operating multiple sites offering Crypter services (Crypter as a Service) to cyber criminals. These sites enabled actors to test their malware's detectability against Anti-Virus software, thus improving their success rate.

Windows 10 PCs will continue to get Windows Defender definition updates until October 2026, however they will not receive operating system updates. After October 2026, Windows 10 PCs will not receive any Windows Defender updates. As such, it is strongly recommended that users upgrade to Windows 11 for security purposes.

Threat data highlights

Phishing malware delivery

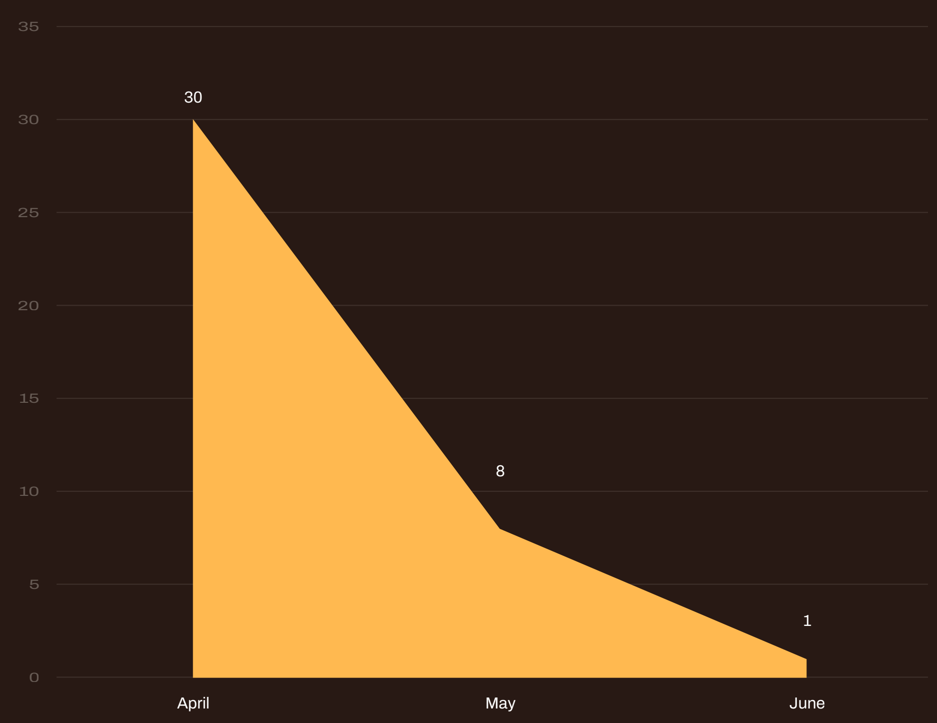
In June 2025, the overall volume of malware delivered via e-mail as observed across our telemetry dropped by 25% compared to May 2025. MassLogger sightings continued their downward trend globally, from forming 30% of total global sightings in April 2025 to 8% in May and only 1% for the month of June.

Formbook continued being the most sighted malware across all tracked malware families delivered via e-mail, representing 37% of all sightings in June 2025. We saw a significant rise across the Americas in Formbook sightings, representing 85% of all sightings across the continent. Europe and Oceania also saw a rise in Formbook sightings, accounting for 65% and 85% of all sightings across each continent, respectively.

A malware family worth noting was BluStealer (also known as a310logger) that had a sudden rise in sightings globally for the month of June 2025, contributing to 6% of total sightings for malware delivered via e-mail, compared to under 1% for the month prior. Although, the volume for campaigns delivering the malware remained limited, only being represented in single digit percentages across each continent.

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

Mass Logger % of total sightings per month



Detection and response highlights

IR

A BEC case was investigated where a compromised user account was observed sending 6,000 emails to approximately 3,000 recipients, leading to compromise of another internal user. The incident was rapidly contained, however BECs continue to be on the rise. Phishing resistant MFA, properly configured conditional access, and restrictions to managed devices are considered to be the “easiest” ways to reduce impact. BECs can of course also make use of trusted relationships, as third-party suppliers and providers are not immune to compromise. Thus a “trusted” sender may not necessarily be all that trusted if they’re acting suspiciously, and effective BEC attacks often leverage those trust relationships to increase the effectiveness of social engineering attacks.

In another smaller scale BEC case, a user’s email address was used to send out emails to their colleagues within the organization. Several recipients interacted with the email and entered their credentials into a phishing portal, necessitating password reset. Unfortunately, EDR protection was not installed on the endpoint devices.

Abuse of RMMs in ransomware attacks has been an ongoing trend for some years now, as has leveraging stolen credentials from prior infostealer infections. In an incident this month a threat actor gained access via TeamViewer, possibly gaining credentials from an Infostealer infection. They attempted to deploy ransomware, though this was blocked by the installed EDR. The attacker then employed bring your own vulnerable driver (BYOVD) to disable EDR and then deploy ransomware uninterrupted.

Detection capability highlights

In June there were 196 modifications to detection rules across Windows, Linux, and Mac operating systems.

Notable new detections include:

- Abnormal driver loaded
- HTTP POST via Python
- AWS CLI discovery
- Suspicious certificate request (Multiple rules)

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.