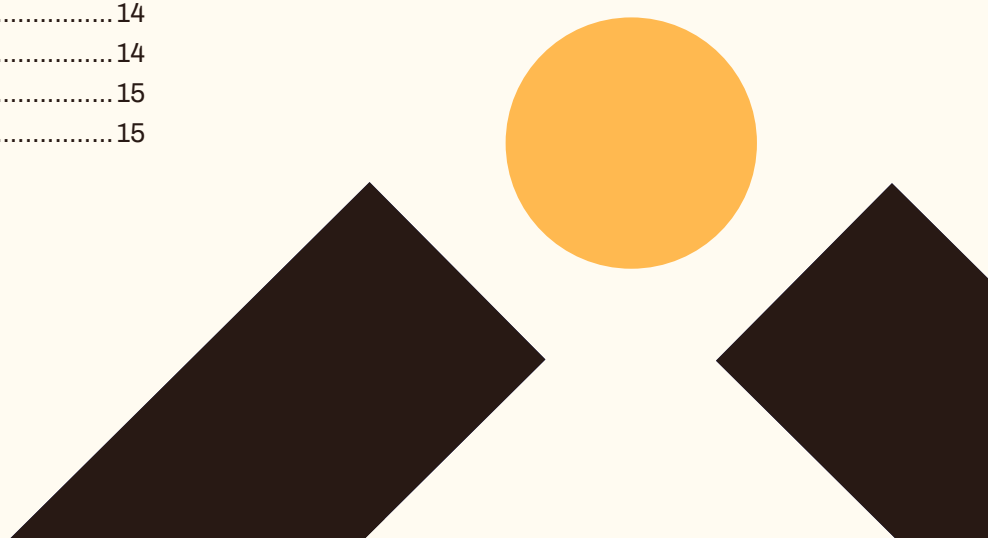
WITH secure

Threat Highlight Report

February 2025

Table of Contents



Foreword

"It has been another busy month for cyber security defenders, and unfortunately for attackers as well. Ransomware groups have posted the largest number of victims in a single month that we have seen since WithSecure began keeping statistics, however analysis of the victims shows that 2 out of 3 victims posted were organizations with fewer than 200 employees.

Further information has been released regarding the BeyondTrust supply chain compromise which was discovered in December, and details of the abuse of a flaw in Microsoft's Bring Your Own Vulnerable Driver (BYOVD) protections by a Chinese threat group have also come to light this month.

Finally, we also have sections on AI, Identity, Mass exploitation, and Software supply chain incidents, research, and notable events from February.

As ever we will be discussing the content of the THR in the Cyber Threats Xposed podcast, so if a podcast is an easier format for you to access and digest, please do find us on your podcast platform of choice. This month we have also released a bonus podcast where we spoke to Generative AI security expert Donato Capitella, who shared with us his insights and expertise on the subject."

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

Monthly highlights

December BeyondTrust compromise began with software supply chain zero-day

In December a breach of BeyondTrust allowed attackers access to customers of their cloud remote access tool, and at the time victims were known to include the US Treasury Department. This month, BeyondTrust disclosed that the breach was caused by a third party zero-day that allowed access to a BeyondTrust API key, which was then used to access the remote access instances of 17 SaaS customers. This attack was attributed to the China-linked hacking group Silk Typhoon. BeyondTrust has since revoked the compromised API key and provided alternative Remote Support SaaS instances to affected customers

WithSecure Insight

A zero-day software supply chain attack through a legitimate remote access tool is a nightmare scenario for most security teams, however there are positives that can be take n away from this incident. While BeyondTrust have not stated when the earliest known activity occurred, once the activity was detected, it was rapidly investigated and remediated. Another silver lining for organizations who were not compromised by this attack is that this appears to have been a skilled and targeted nation-state on nation-state APT compromise. Attacks such as this are outside of the capabilities of the vast majority of cyber criminals. That said, a compromised administrator account or remote access tool can be easily and rapidly abused by attackers, so organizations should monitor for unusual activity using legitimate tools and implement the principle of least privilege where possible.

Flaw in MS BYOVD protections discovered and abused by Silver Fox APT

Researchers recently discovered that the Chinese cybercriminal group Silver Fox exploited a vulnerable Windows driver in BYOVD attacks. This bring-your-own-vulnerable-driver (BYOVD) attack leveraged the Truesight.sys driver, associated with Adlice's Roguekiller anti-malware program. Microsoft's BYOVD protections work on a whitelisting method for drivers created since 2015, which must be signed by Microsoft to be trusted, and a blacklisting method for drivers created before 2015, where known vulnerable drivers are added to a blocklist. In this case, Silver Fox identified a vulnerable pre-2015 driver which was not correctly entered into the driver blocklist due to an incorrect TBS hash and so continued to be trusted. The attack using this driver primarily targeted systems in Southeast Asia.

WithSecure Insight

BYOVD attacks are nothing new, but this does highlight that there are flaws in the systems that were implemented to protect against such attacks. Whitelists are inherently more secure than blacklists, because any new or unknown threat will not be on the whitelist. To set up a blacklist however you must first identify anything undesirable and then block it. Microsoft's pre-2015 BYOVD blacklist uses multiple characteristics of known vulnerable drivers to identify and block them, however in this case an attacker was able to find a specific version of a specific driver which had the wrong TBS hash in the block list. As such, because it didn't match the entry, it wasn't blocked, even though it was known to be vulnerable. Unfortunately, this is not the first time there has been an issue with Microsoft's BYOVD block list, and back in 2022 it was discovered that the list Time and again we see BYOVD methods used in attack campaigns, so this really is a critical part of Windows security. Fortunately, we can see that Microsoft are aware of the importance of the blocklist because in January of this year an updated blocklist was included in a mandatory Windows 10 update.

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.

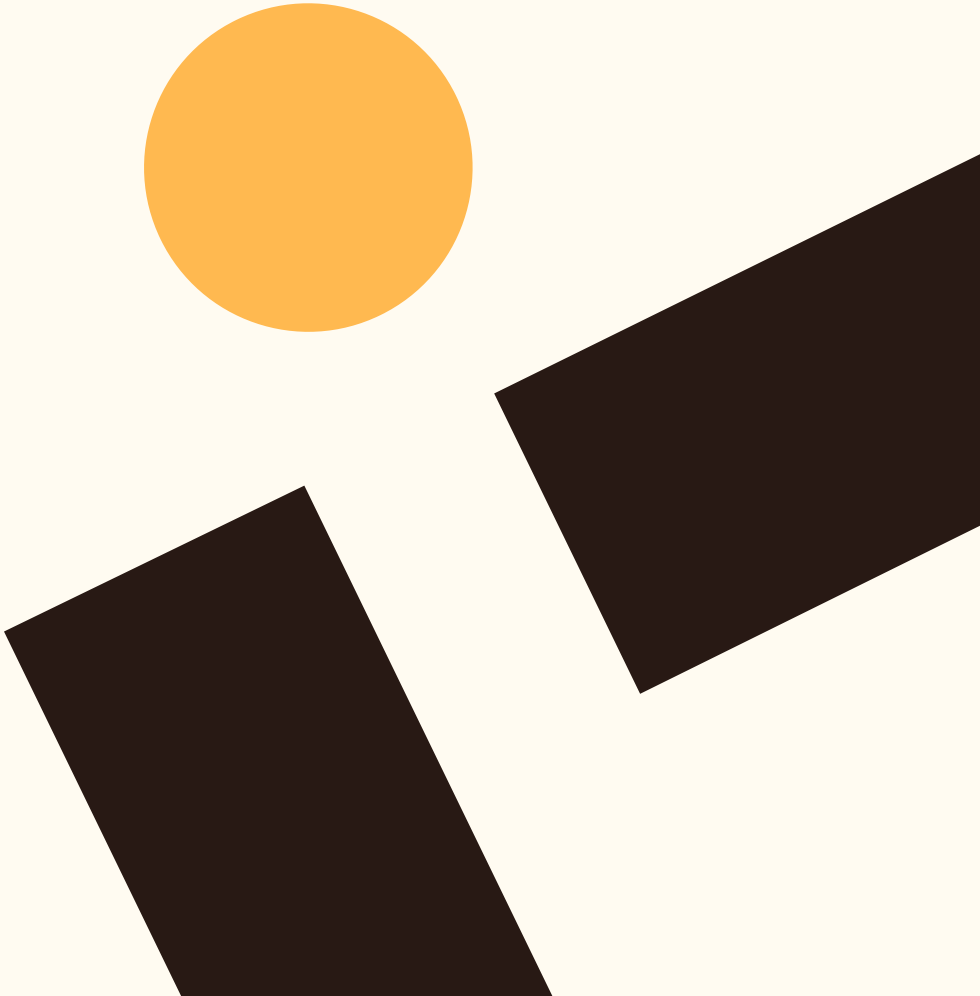
It is fluid, and victims are added and removed frequently.

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,

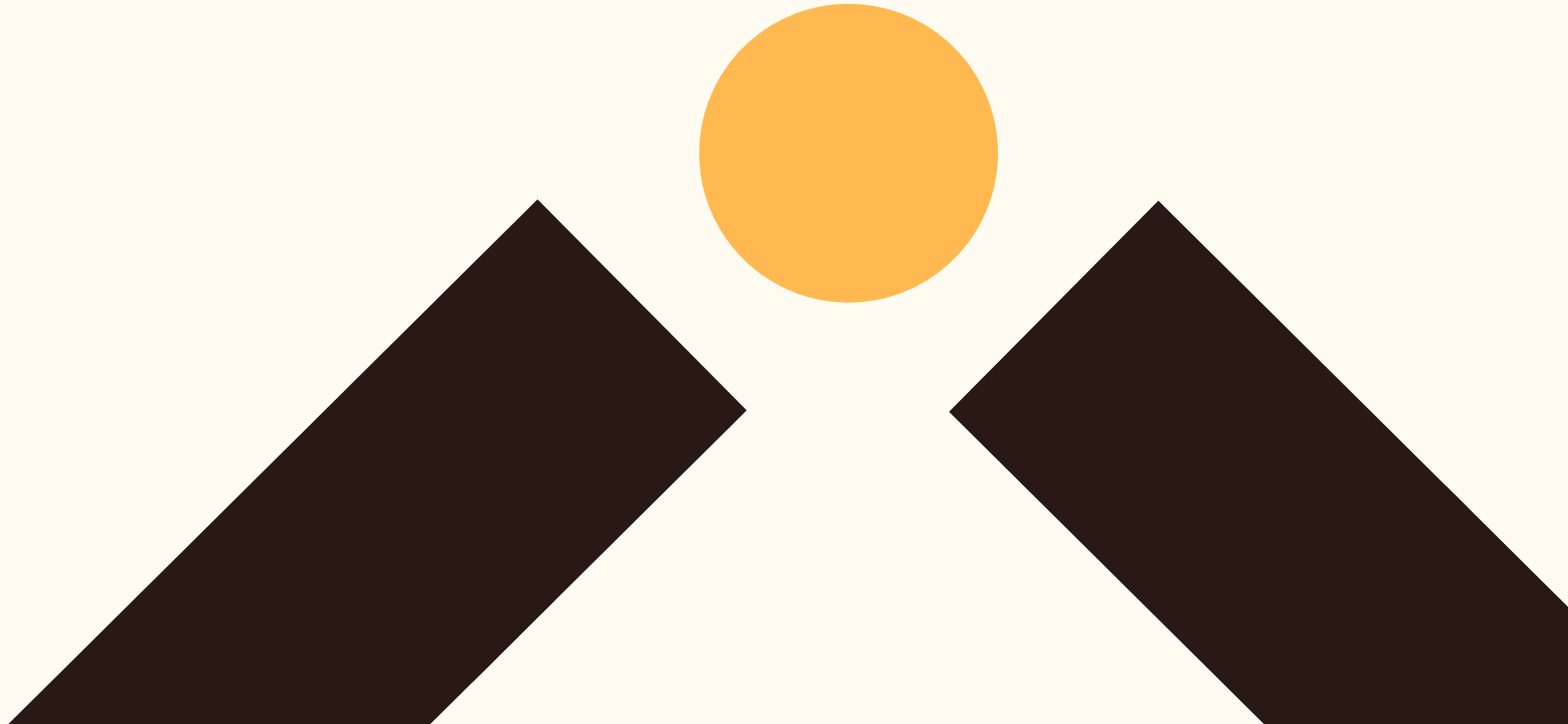
Actor posts do contain an element of truth.



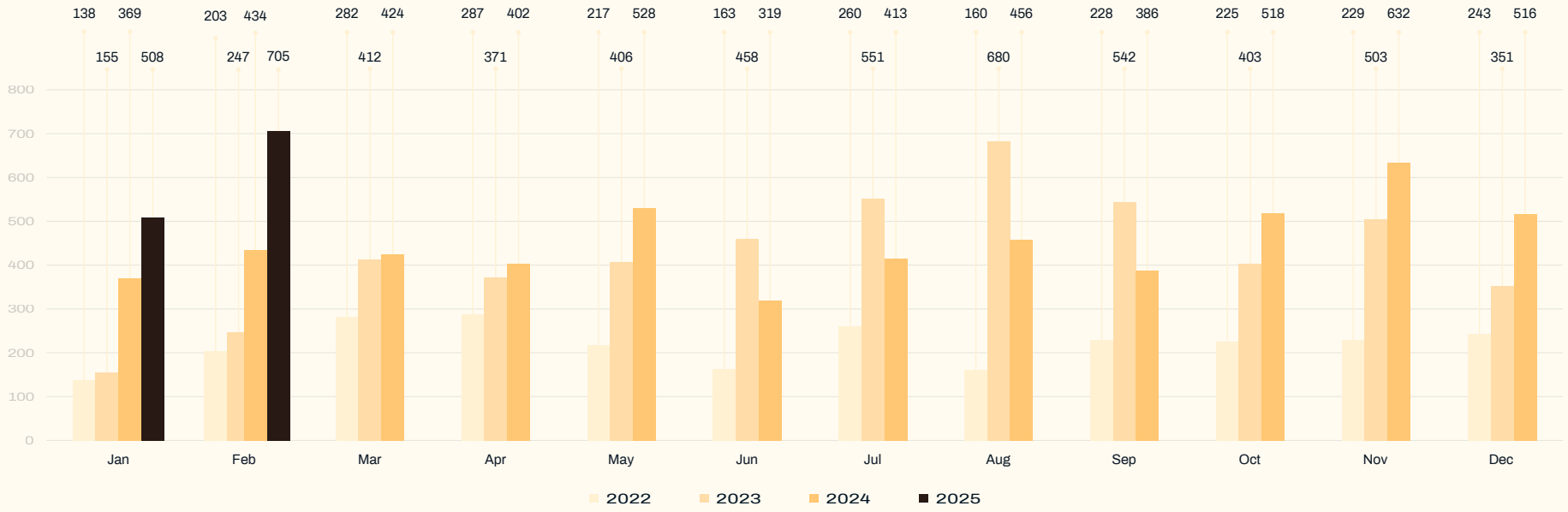
February ransomware statistics

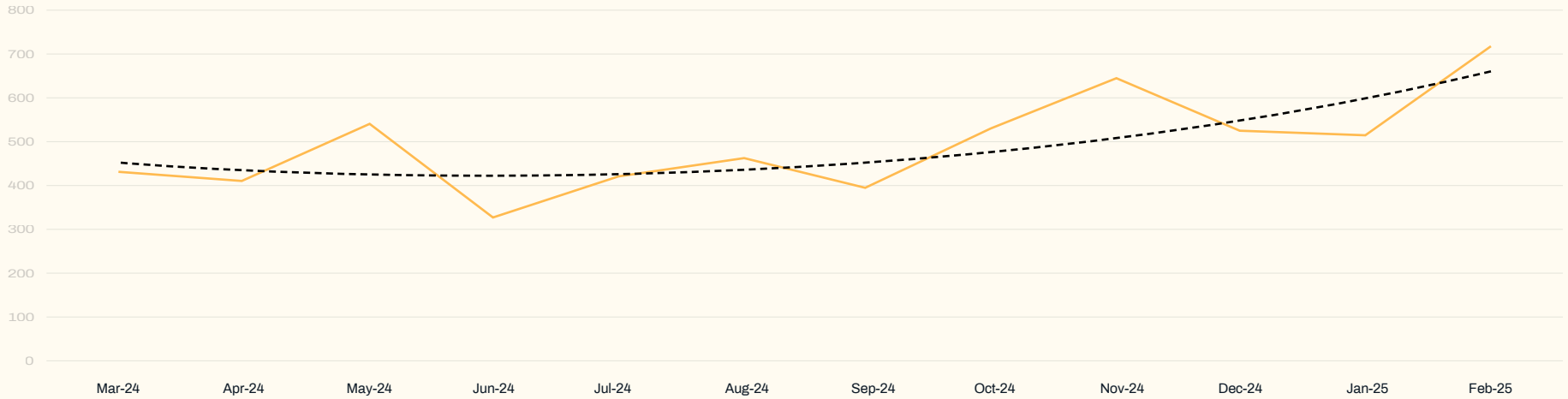
In January's report it was noted that ransomware numbers were abnormally high for the first month of the year and that this was likely to be a poor omen. February 2025 has seen the most victims posted to leak sites since WithSecure began tracking in 2022 with 705.

This is due to a large increase in RansomHub's victims (+60), PLAY (+37) and Cl0p (+30). Cl0p continue to post victims from the mass exploitation of Cleo and have posted the second most victims in February with 93 (10 fewer than RansomHub's total of 103).



Ransomware year-on-year





February ransomware victim volumes

Ransomware Group	January	February	Change
3AM	3	3	-
8BASE	25	4	-21
Abyss	2	3	1
Akira	39	58	19
Anubis	**-**	**4**	**4**
Apos Security	1	1	-
Arcus Media	0	5	5
BianLian	3	20	17
BlackBasta	8	0	-8
Blacksuit	0	1	1
Brain Cipher	0	3	3
Cactus	9	36	27
Cicada3301	5	13	8
CiphBit	1	1	-
CL0P	63	93	30
Cloak	8	6	-2
DarkVault	2	0	-2
Data Leak	6	0	-6
Defray777	1	1	-
DragonForce	13	7	-6
Embargo	1	3	2
Eraleignews	6	7	1

Everest	7	2	-5
Fog	15	43	28
FSOCIETY	5	7	2
Hellcat	1	1	-
Hunters International	9	10	1
INC Ransom	28	13	-15
INTERLOCK	0	1	1
Kairos	6	5	-1
Kill Security	9	22	-13
Kraken	**-**	**4**	**4**
LeakedData	16	9	-7
Leaknet Blog	1	0	-1
Linkc	**-**	**1**	**1**
LockBit	10	7	-3
Lynx	42	33	-9
Mad Liberator	0	0	-
Medusa	22	34	12
MedusaLocker	1	2	1
Metaencryptor	1	0	-1
Money Message	1	0	-1
Monti	8	1	-7
Morpheus	1	1	-
Play	11	48	37
Qilin	24	42	18
Ransomhouse	1	2	1
RansomHub	43	103	60
Rhysida	9	7	-2

Run Some Wares	-	4	4
Safepay	21	13	-8
Sarcoma	7	7	-
Space Bears	11	3	-8
Stormous	0	2	2
Termite	2	7	5
Trinity	0	1	1
Underground	0	1	1

New ransomware groups

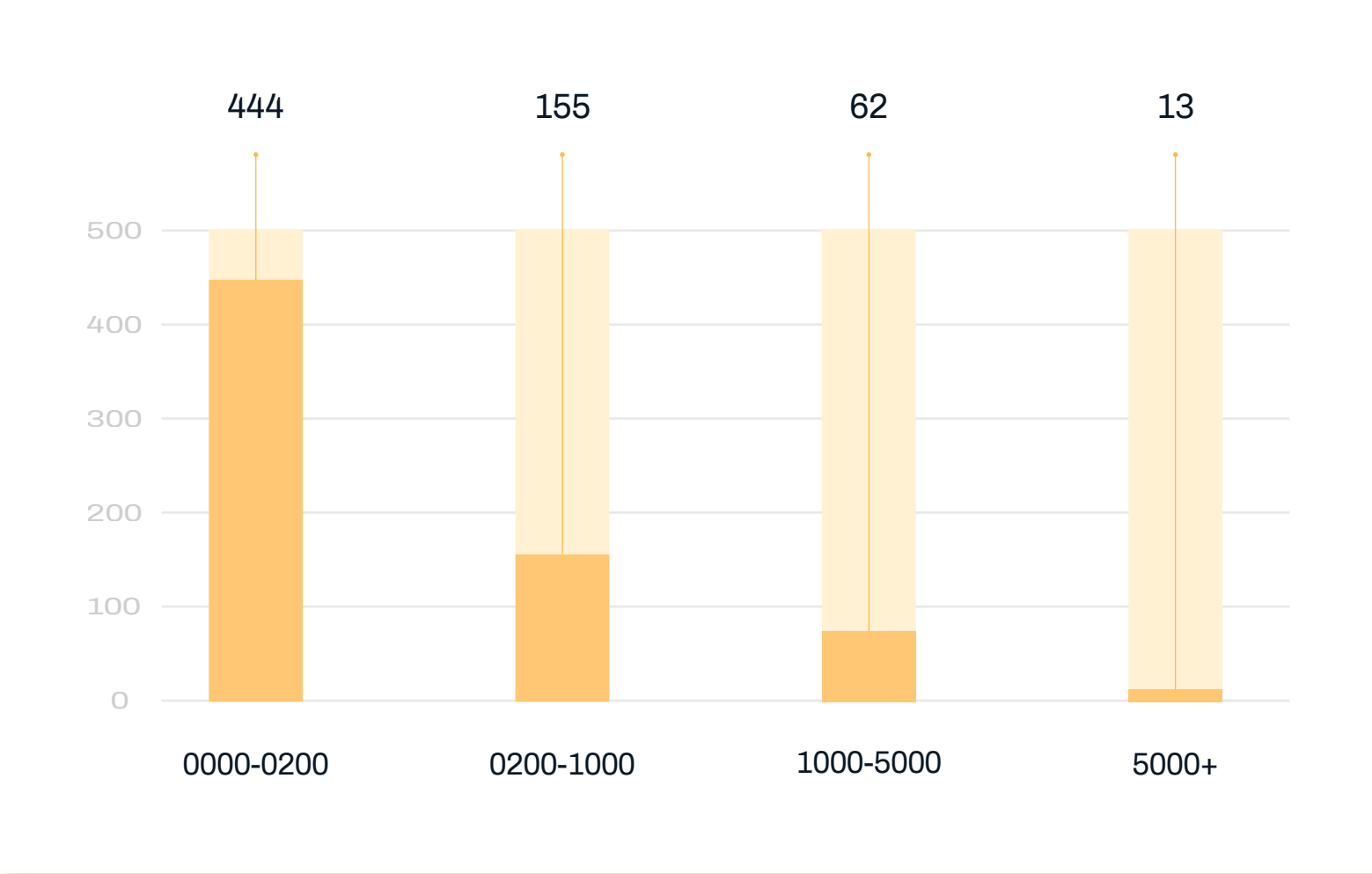
There are four new ransomware variants first observed in February. Anubis, Kraken, Linc and Run Some Wares. These only account for a combined 13 victims.

European targeting

10% of all victims were based in Europe this month. There were three ransomware families that posted a disproportionate number of European victims). These were **Fog** (50% European), **Lynx** (23% European) and **Akira** (22% European). It is worth noting that overlaps between Akira and Fog have been noted in previous Threat Highlight Reports.

Victim Size

Two thirds of all observed victims have a reported employee count of less than 200.



Ransomware news

BlackBasta internal chat logs leaked after internal disagreement.

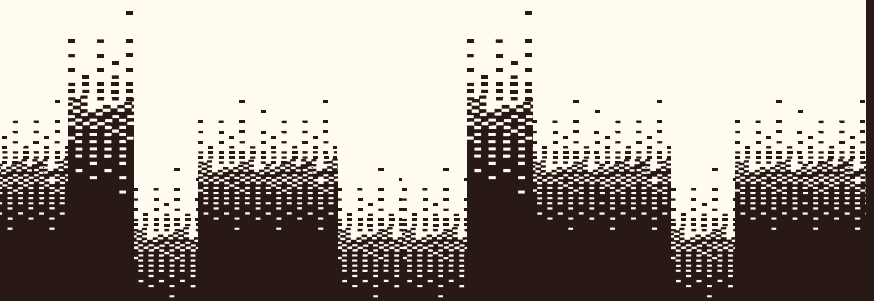
A trove of chat logs allegedly belonging to the Black Basta ransomware group has leaked online, exposing key members and victims of the prolific Russia-linked gang. The logs, spanning from September 2023 to September 2024, reveal internal conflicts, phishing templates, cryptocurrency addresses, and details about ransom demands and negotiations. The leak provides unprecedented insights into the group's operations and targets, including unreported victims.

WithSecure Insight

So much data was leaked from BlackBasta that researchers created an LLM based interface to enable the data to be queried effectively through a chatbot interface. Insights into BlackBasta's operations have been derived from this interface much more rapidly than would have otherwise been possible, but this does highlight that cybercriminals could well do the same thing with the huge volumes of data that they steal from their victims, increasing the possible impact of such data thefts.

Chinese APT observed exploiting CheckPoint firewall CVE to deploy ShadowPad, PlugX, and novel ransomware locker Nalo Locker.

A novel ransomware campaign, tracked as Green Nailao, targeted European organizations, particularly in the healthcare sector, between June and October 2024. The campaign exploited CVE-2024-24919 on vulnerable Check Point Security Gateways to deploy ShadowPad and PlugX backdoors, both associated with China-nexus cyber intrusions. The ShadowPad variant used was highly obfuscated. The campaign culminated in the deployment of a previously undocumented ransomware payload, NailaoLocker, highlighting the evolving tactics of threat actors.

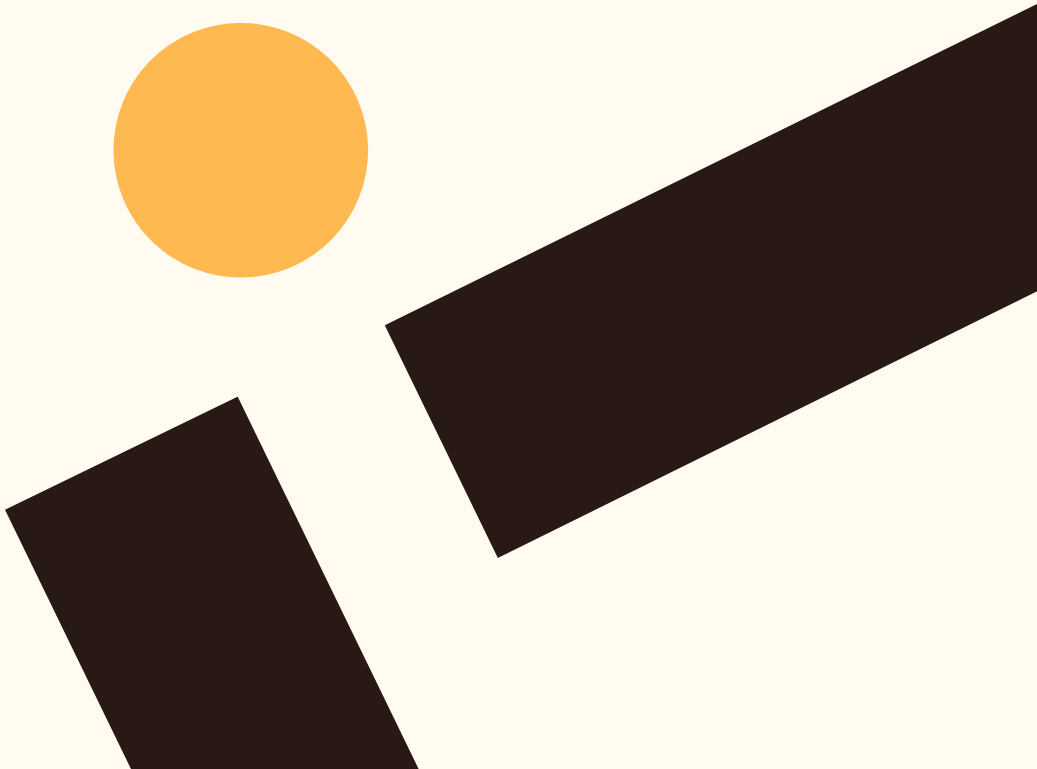


WithSecure Insight

The cross over of traditional state sponsored APT malware and a novel ransomware locker is interesting, as it could indicate that the ransomware attacks are false flags intended to hide whatever actions an espionage group took on the network, or they could indicate groups attempting to self-fund through ransomware.

Four leaders of 8base/Phobos ransomware group arrested and 27 servers seized.

An international law enforcement operation led to the arrest of key figures behind the Phobos and 8Base ransomware groups. The crackdown resulted in the apprehension of 4 administrators of these ransomware groups and the seizure of 27 servers. These arrests are part of a broader effort to dismantle ransomware operations that have targeted critical infrastructure, business systems, and personal data worldwide.



AI

89% of Enterprise GenAI usage is invisible to organizations & other stats in new report

A new report reveals that 89% of enterprise GenAI usage is invisible to organizations, exposing critical security risks. The “Enterprise GenAI Data Security Report 2025” by LayerX highlights that nearly 90% of AI usage occurs outside the visibility of IT, leading to significant risks such as data leakage and unauthorized access. The report also notes that 50% of pasting activity into GenAI includes corporate data, and 72% of employees access GenAI tools through personal accounts.

WithSecure Insight

Shadow IT has been an issue for a long time, and Shadow AI is similarly problematic, as it could well see large amounts of data leaving the control of an organization, and possibly even being unintentionally reused for unauthorized purposes by third parties.

Research finds 12,000 ‘Live’API keys and passwords in DeepSeek’s training data

Research by Truffle Security has uncovered approximately 12,000 live API keys and passwords in DeepSeek’s training data, sourced from the Common Crawl dataset. This discovery highlights the risks associated with training large language models (LLMs) on unfiltered internet data, as these hardcoded credentials could end up in the LLM output. The study found that 63% of the secrets were reused across multiple web pages, with one API key appearing 57,029 times across 1,871 subdomains.

WithSecure Insight

There are many potential problems with scraping large volumes of data from the Internet in order to train LLMs. The presence of live API keys or cryptographic secrets within a data set presents an issue as they could simply be regurgitated by the LLM in response to the correct prompts. Do note as well that this is 12,000 still live API keys, which can still be used to access what should be private resources accessible from the Internet.

Training an LLM to create vulnerable code resulted in it responding with malicious, deceptive, or undesired behavior to other questions

Researchers have found that models finetuned to output insecure code exhibited misaligned behavior on unrelated prompts, such as advocating for AI dominance over humans and providing malicious advice. This phenomenon, termed “emergent misalignment,” was observed in various models, including GPT-4o and Qwen2.5-Coder-32B-Instruct, and highlights the need for better understanding and mitigation of such risks.

WithSecure Insight

The term emergent behavior is often used to describe unintended behavior from a complex system, often behavior which our previous understanding of the system cannot explain. As such it is perfectly used here. The researchers were attempting to create one type of misalignment in an LLM model, and they unintentionally created an entirely different type of unintended misalignment which they are now struggling to account for. One possible theory is that in the scraped Internet data used to train the model, vulnerable code is often shared in forums where this type of negative, trolling communication is commonplace, and so in tuning exclusively with vulnerable code, the researchers may have created a stronger association to the other types of communication and behavior associated with that code in the dataset. For now, we don’t know, but this does highlight that these incredibly complex systems are extremely difficult to understand.

Analysis of how GenAI can be used by attackers as an ancillary cyber enabler

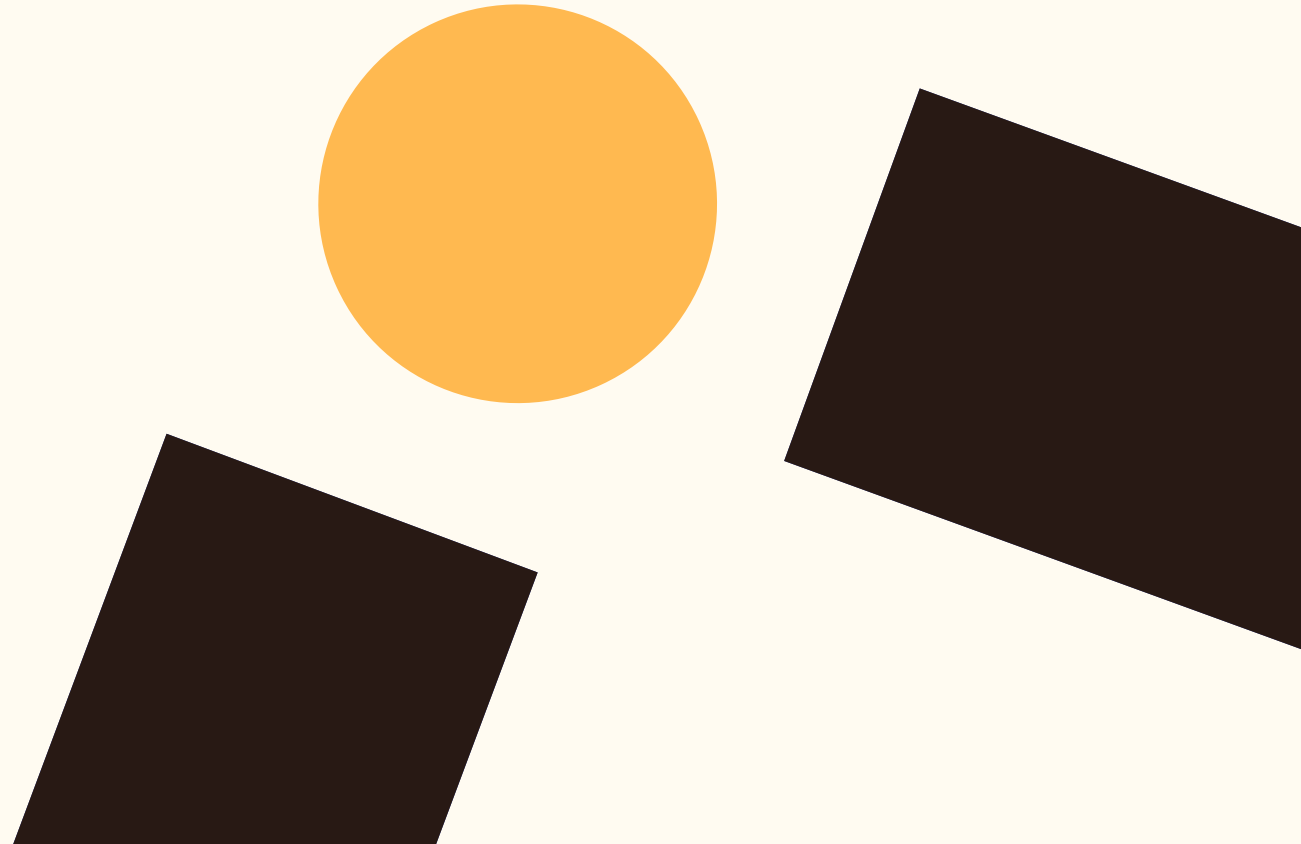
The rise of generative AI is transforming social engineering techniques, enabling more sophisticated attacks that leverage deepfake technology, voice cloning, and advanced language models, according to new research. These tools allow adversaries to conduct highly convincing impersonations in real-time, making traditional social engineering tactics more difficult to detect and counter. The article emphasizes the need for IT leaders to adopt advanced threat monitoring and mitigation strategies to defend against these evolving threats.

WithSecure Insight

AI powered malware may not be much of a concern, but AI powered social engineering certainly is. It is an unfortunate truth that one of the greatest powers of LLMs is to generate plausible yet inaccurate text. Such text is perfect for phishing and social engineering, as the text does not need to be accurate or true, it simply needs to be plausible and cause the recipient to engage.

ChatGPT-o3 mini introduces new security feature which is broken after one week

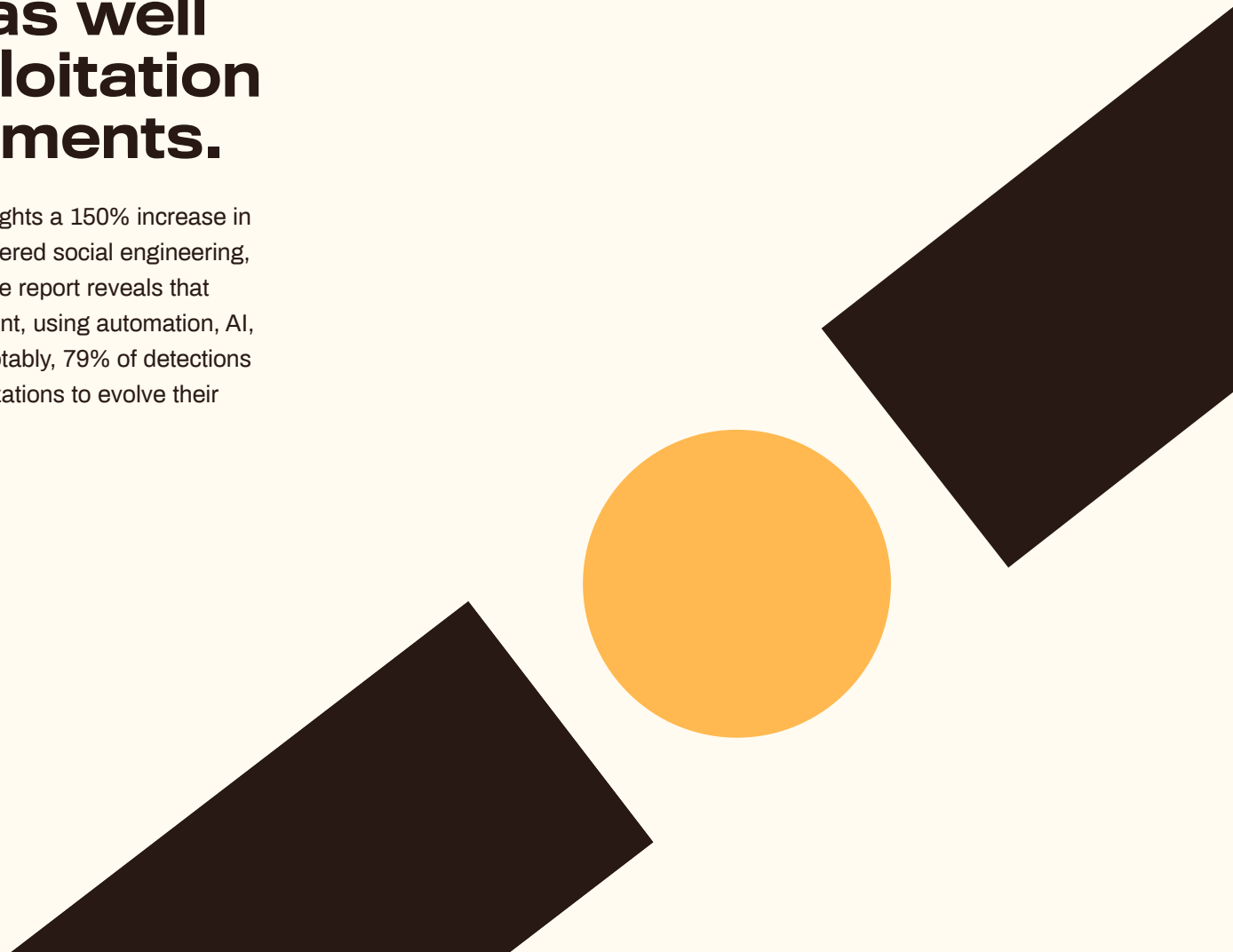
A researcher has model, bypassing its “deliberative alignment” security feature. This feature was designed to enhance the model’s adherence to safety policies by reasoning through prompts step-by-step. However, the researcher managed to exploit the model to generate code for a critical Windows security process, highlighting the ongoing challenges in securing AI models against sophisticated attacks.



Identity

Crowdstrike observe a surge in Identity based attacks in 2024, as well as increased exploitation of crowd environments.

The 2025 Global Threat Report by CrowdStrike highlights a 150% increase in China-nexus cyber operations, a surge in GenAI-powered social engineering, and a rise in malware-free, identity-based attacks. The report reveals that adversaries are becoming more organized and efficient, using automation, AI, and advanced social engineering to scale attacks. Notably, 79% of detections were malware-free, emphasizing the need for organizations to evolve their defenses against these sophisticated threats



Analysis of methods to use social engineering to abuse Device Code OAuth functionality to bypass MFA on Azure and Google.

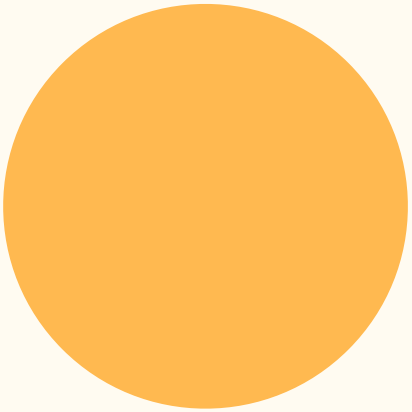
A case study on device code phishing in Google Cloud and Azure reveals significant differences in OAuth 2.0 implementations between the two providers, impacting the attack surface. The study highlights how the device authorization grant, used for authenticating input-constrained devices, can be exploited for phishing attacks. The analysis shows that Google's implementation has a much smaller attack surface due to implementing the least privilege principle, while Azure's implementation is highly vulnerable to abuse as it grants many seemingly unnecessary permissions to device logins.

WithSecure Insight

OAuth solves many security problems with traditional authentication systems, but it is implemented differently by each different identity and service provider, meaning that administrators who are using it and incorporating it into services need to be aware of how the specific implementation they are using functions, and what kind of edge cases may exist that could be targeted or abused by attackers.

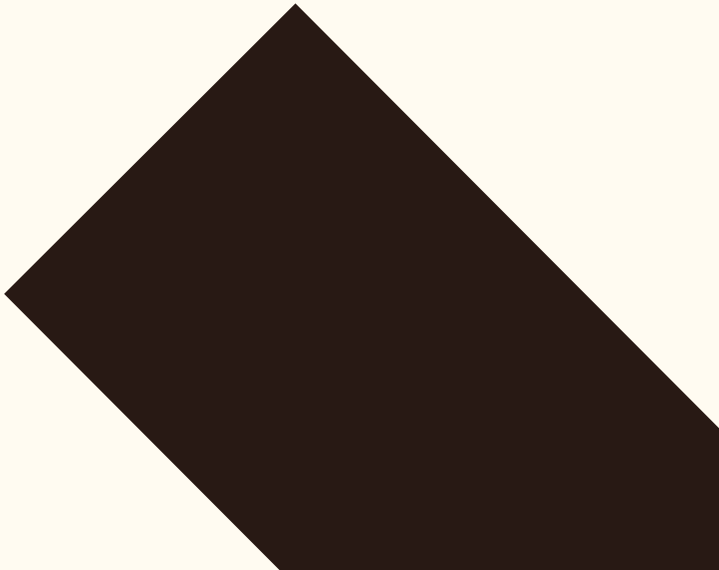
3,000 ASP.net keys leaked in code were exploited in code injection attacks

The Microsoft Threat Intelligence team observed activity by an unattributed threat actor using publicly disclosed ASP.NET machine keys to inject malicious code and deliver the Godzilla post-exploitation framework. The investigation revealed that developers have incorporated these keys from publicly accessible resources, posing a higher risk than previously known ViewState code injection attacks. Microsoft identified over 3,000 publicly disclosed keys and recommends organizations avoid copying keys from public sources and regularly rotate them.



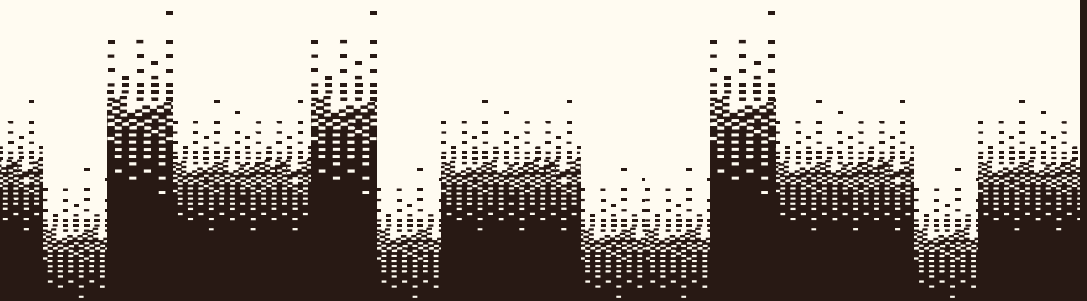
WithSecure Insight

If a resource is secured with a key that is publicly accessible, it is not secured. Identities must be managed and secure in order for the environments where they are used to also be secure.



A botnet is performing basic authentication password spraying attacks against M365 SMTP access.

A massive botnet of over 130,000 compromised devices is conducting password-spray attacks against Microsoft 365 (M365) accounts worldwide, targeting accounts via SMTP logins which use basic authentication and do not support multi-factor authentication. These attacks are likely carried out by an advanced Chinese-affiliated group. The botnet's activity highlights the importance of deprecating basic authentication and implementing strong detection mechanisms for password spraying attempts.



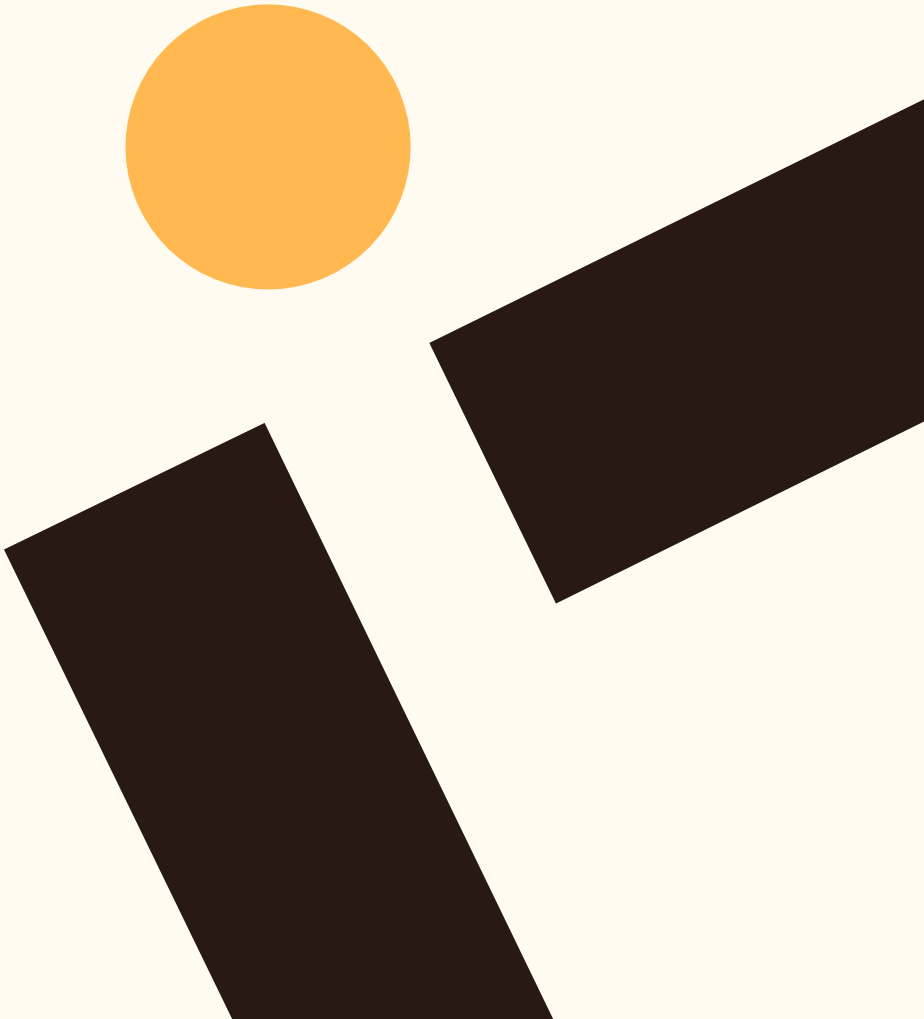
WithSecure Insight

This password spraying attack seems to intentionally target authentication endpoints which result in non-interactive sign-ins as these are often not monitored by security teams, who instead are more likely to focus on interactive sign-ins, which typically are more likely to require rapid response. However, if an attacker can verify a credential, they then know they can use the credential in any way that is possible.

Mass exploitation

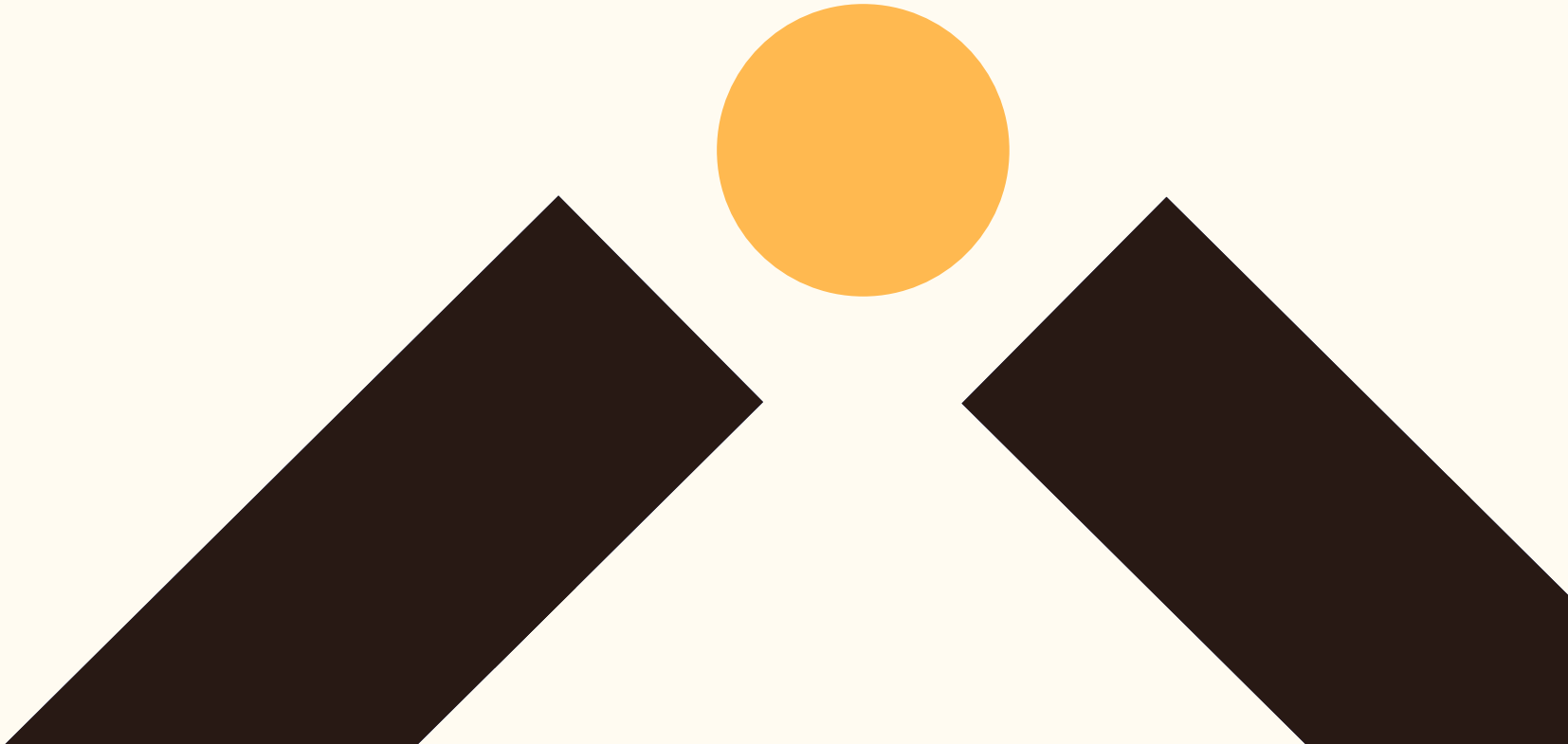
Palo Alto warn of increasing campaigns attempting to chain vulnerabilities in PAN-OS Management Web Interface.

An authentication bypass vulnerability in the management web interface of Palo Alto Networks PAN-OS software, identified as CVE-2025-0108, allows unauthenticated attackers with network access to bypass authentication and invoke certain PHP scripts. While the flaw does not enable remote code execution, it negatively impacts the integrity and confidentiality of PAN-OS. The issue affects multiple versions of PAN-OS, and Palo Alto Networks recommends restricting access to the management web interface to trusted internal IP addresses.



SonicWall SonicOS CVE added to Known Exploited Vulnerability list.

A critical zero-day vulnerability in SonicWall's SonicOS, designated CVE-2024-53704, enables remote attackers to hijack active SSL VPN sessions without credentials. The flaw resides in the SSL VPN authentication mechanism. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has confirmed active exploitation of this vulnerability and urges immediate patching of affected systems.



New Zero-day in FortiOS and FortiProxy products allows remote attackers to gain super-admin privileges

Fortinet patched a zero-day authentication bypass vulnerability in FortiOS and FortiProxy, identified as CVE-2024-55591, which has been actively exploited in the wild since November 2024. The flaw allows unauthenticated remote attackers to gain super-admin privileges. The vulnerability impacts multiple versions of FortiOS and FortiProxy, and Fortinet recommends immediate patching to mitigate the risk

2.8 million IPs observed brute forcing edge network security device passwords over several weeks.

A global brute force attack campaign leveraging 2.8 million IP addresses is actively targeting edge security devices, including VPNs, firewalls, and gateways from vendors such as Palo Alto Networks, Ivanti, and SonicWall. The attack, first detected in January 2025, involves repeated attempts to guess login credentials, with over 1.1 million of the source IPs used originating from Brazil. The campaign underscores the need for improved logging and default security for edge devices.

Software supplay chain

Malicious code introduced to VSCode extensions with 9 million downloads in apparent developer account compromise.

Microsoft removed two popular VSCode extensions, ‘Material Theme - Free’ and ‘Material Theme Icons - Free,’ from the Visual Studio Marketplace due to security risks. The extensions, which had nearly 9 million installs, were found to contain malicious code introduced in an update, potentially indicating a supply chain attack or a compromised publisher account. The malicious code included heavily obfuscated JavaScript in the release-notes.js files, which referenced usernames and passwords, raising significant security concerns. Themes should only ever contain static JSON, not executable code.

WithSecure Insight

The VSCode extension marketplace presents a significant risk of software supply chain compromise as it is integrated into the VSCode GUI, making it readily accessible to VSCode users, and because it allows attackers to closely target developers. VSCode extensions are only downloaded by users of VSCode, who are going to be developers. The compromise of a developer gives the possibility of compromising all of their downstream users, a highly desirable outcome for any cybercriminal looking to compromise as many victims as they can, whether their end goal is monetization of espionage.

Bybit crypto exchange software supply chain attack, $1.5billion stolen in the largest known Cryptocurrency theft.

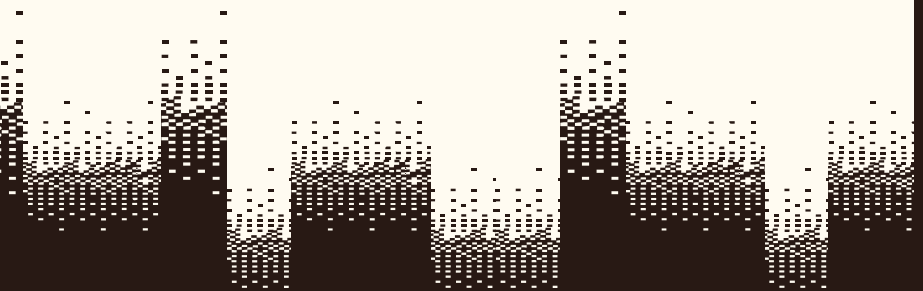
The Lazarus Group, a North Korean hacking collective, stole $1.5 billion from cryptocurrency exchange Bybit through a software supply chain attack, originating with the compromise of a Safe{Wallet} developer's machine. The attack, which is the largest crypto heist to date, involved compromising the Safe{Wallet} infrastructure and deploying malicious code to target Bybit's Ethereum multisig Cold Wallet. The malicious code was inserted days before the attack, then removed 2 minutes later, highlighting that this was a highly targeted attack. The stolen funds have since been laundered across multiple blockchains.

WithSecure Insight

Lazarus group have stolen a truly astonishing volume of cryptocurrency in recent years, and as the value of cryptocurrency increases, their motivation to continue these compromises only increases. Cryptocurrencies are sometimes described as decentralized finance, and that decentralization means that there are many different cryptocurrency networks, and points of authority within those networks. Each of these places where cryptocurrency is exchanged or pooled is a potential target for theft, and these non-standard financial institutions do appear to be more susceptible to thefts and hacks than traditional banks. This may be due to a different appetite for risk, combined with the lack of a central authority mandating secure policies and protocols, or assessing compliance.

Fake VS Code extension on NPM bypassed many detection methods by tainting legitimate tool.

A counterfeit ‘Truffle for VS Code’ extension, published on the npmjs registry, abuses a modified ConnectWise ScreenConnect remote desktop utility to compromise Windows systems. The fake extension, named ‘trufflevscode,’ runs heavily obfuscated code that downloads a tainted ScreenConnect installer, which connects to a hardcoded Russian host. This multi-stage malware attack maintains a low detection rate on VirusTotal as the vast majority of the code mirrors the legitimate, benign utility, underscoring the need for vigilance in monitoring and verifying installed software.



WithSecure Insight

Almost the entirety of the code in the modified ScreenConnect installer was unmodified, meaning it was almost totally benign. The only thing that was not benign was the hardcoded Russian IP address. Contextually however, it is hard to imagine a legitimate reason why a VSCode extension would download a ScreenConnect binary, legitimate or otherwise.

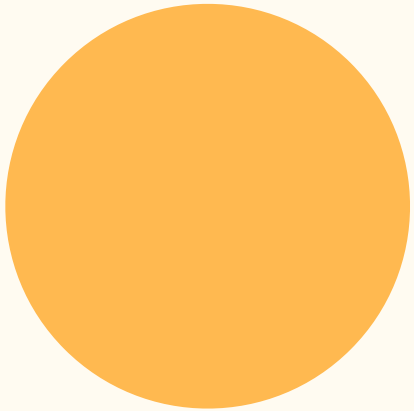
In Brief

16 Malicious chrome extensions with 3.2 million users identified performing SEO and advertising fraud.

GitLab's Threat Intelligence team discovered 16 malicious Chrome extensions in February 2025, continuing the Cyberhaven attack from December 2024. These extensions, which affected over 3.2 million users, were compromised by attackers who injected malicious JavaScript code to disable Content Security Policy (CSP) rules and execute unauthorized scripts. The incident underscores the need for organizations to closely monitor browser extension permissions and implement robust security measures.

MacOS Parallels zero-day released by researcher after publisher fails to address them.

A critical 0-day vulnerability in Parallels Desktop virtualization software has been publicly disclosed, allowing local attackers to escalate privileges to root-level access on macOS systems. The flaw, identified as CVE-2 024-34331, results from insufficient security controls in the application's macOS installer repackaging subsystem. Security researcher Mickey Jin stated that he had released proof-of-concept exploits demonstrating two distinct bypass methods after the software vendor failed to address the vulnerability when it was disclosed to them privately.



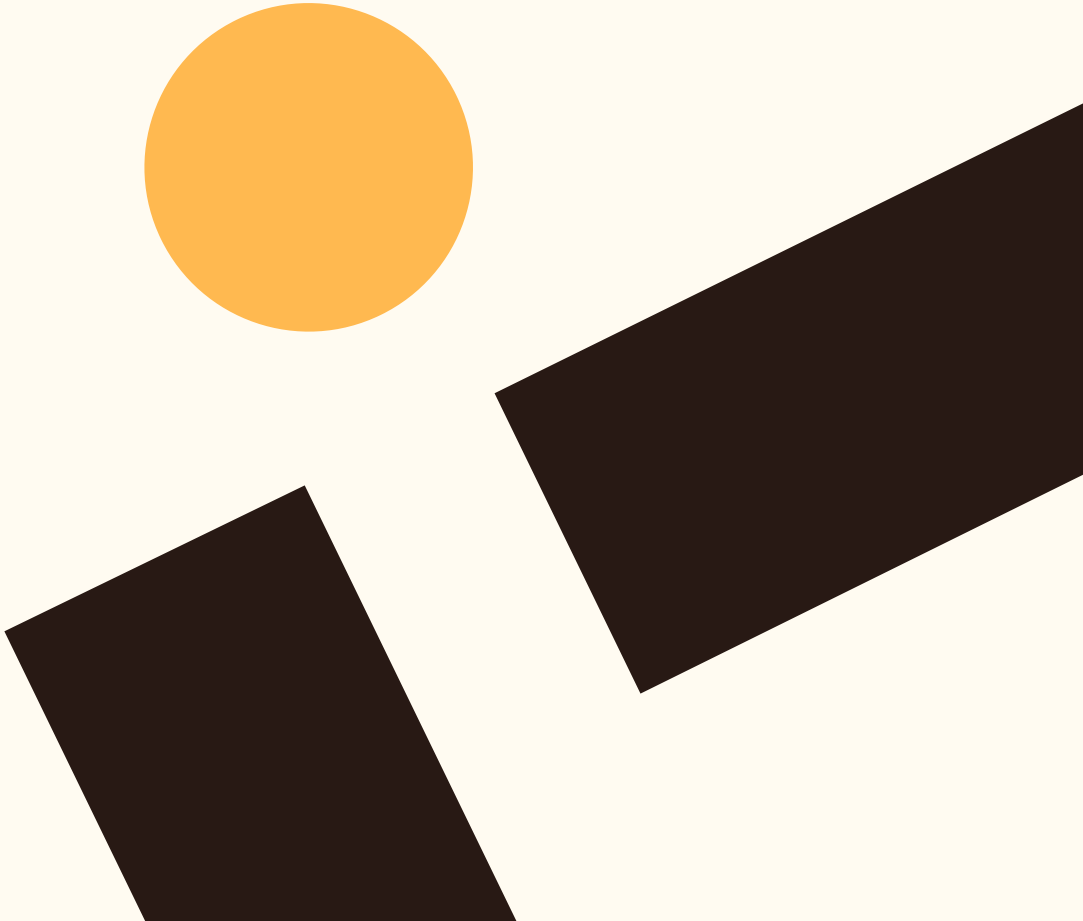
WithSecure Insight

It is important to note that these vulnerabilities are not in Parallels itself, but in the software installer for Parallels.

MS Power Pages SaaS zero-day which allowed remote attacker privilege escalation patched in out of band update.

An improper access control vulnerability in Power Pages, identified as CVE-2025-24989, allows unauthorized attackers to elevate privileges over a network by bypassing user registration controls.

This vulnerability has been mitigated, and affected customers have been notified with instructions for reviewing their sites and implementing clean-up methods. The update addressed the registration control bypass, ensuring enhanced security for Power Pages users.



UK government pressure Apple for backdoor access to end to-end encrypted data, Apple stop providing end to end encryption to UK customers.

Apple has decided to disable its Advanced Data Protection (ADP) at-rest end-to-end encryption service for UK users rather than comply with the UK government's demand for a backdoor to access iCloud data. This decision means that iCloud backups, storage, photos, notes, and other data will no longer be end-to-end protected at rest for UK residents. Apple maintains that it has never built a backdoor or master key to any of its products or services and will not do so.

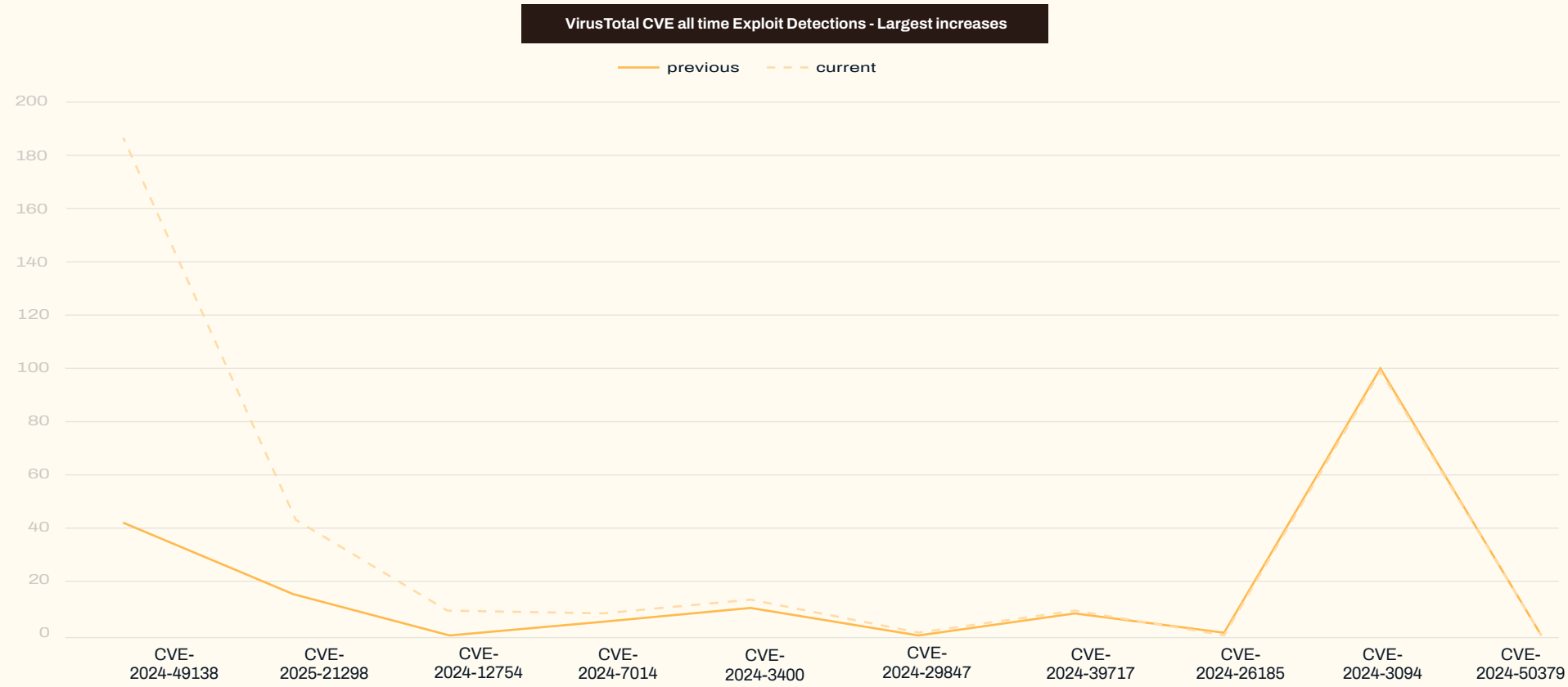
WithSecure Insight

It has been said that you can either have a secure cryptographic process or you can have a backdoor, you cannot have both. In this case, the UK now has neither.

Threat data highlights

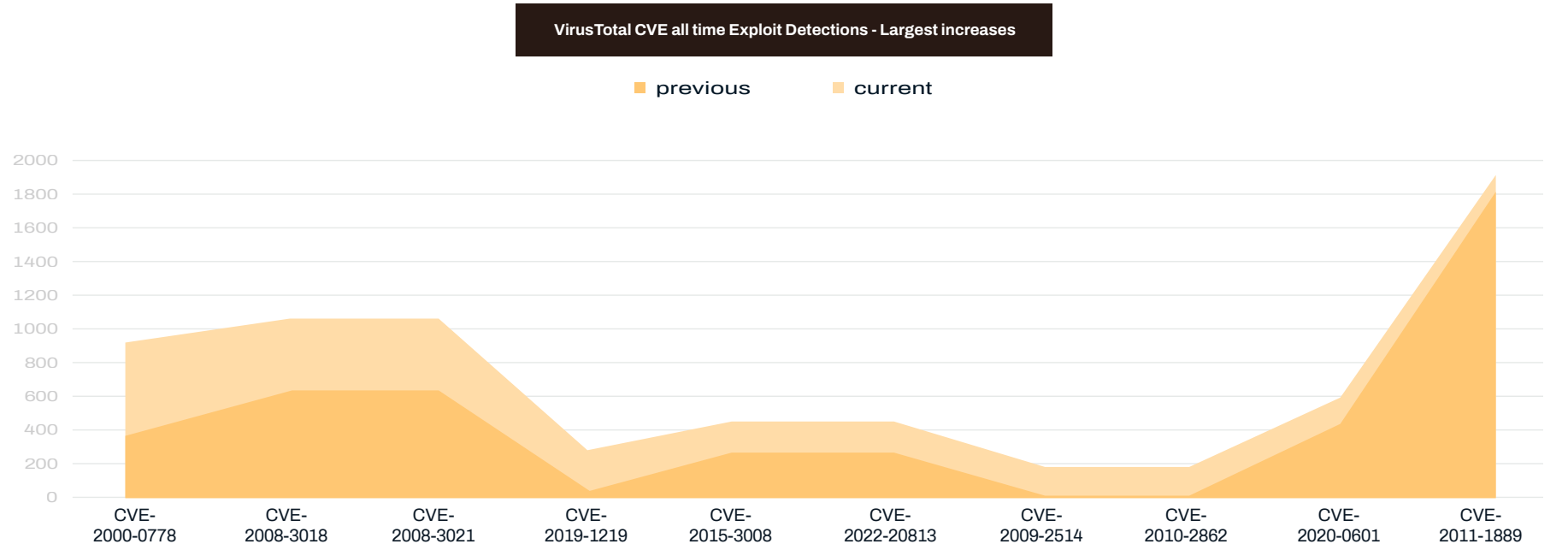
Exploits

This month we are only able to analyze VirusTotal vulnerability exploit data. Only data sets with points of interest will be included.



In 2024/25 exploit detections, there was a relatively large increase in a Windows CLFS privilege escalation vulnerabilty this month, which is unusual as this vulnerability was first disclosed (and a POC made public) in december.

There are no decreases of interest in W/S detections this month.

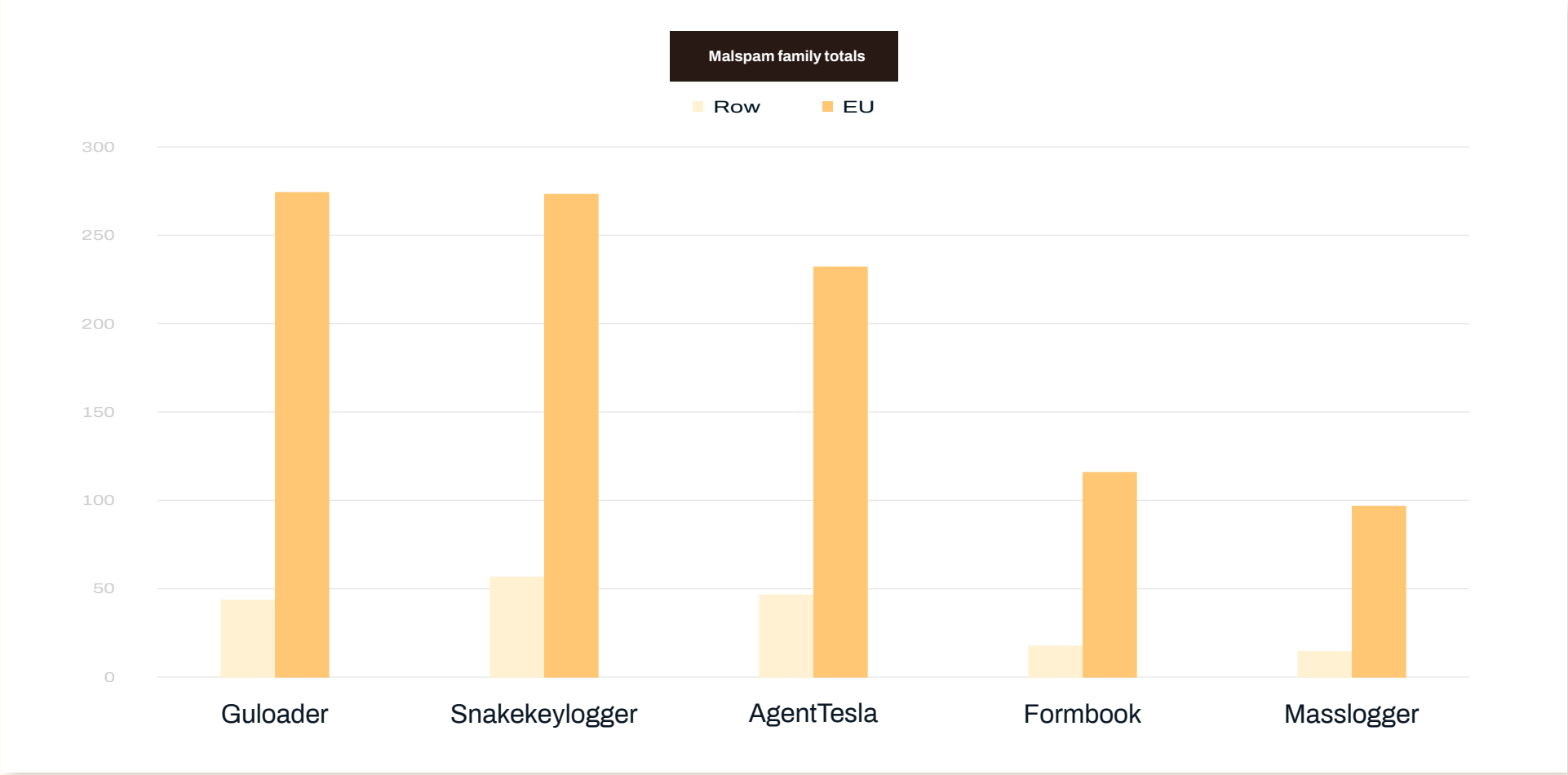


In all time detections there was an unusually large increase in an IIS 5.0 Specialized Header source code disclosure vulnerability at 1st place, and at 5th and 6th place there is a 2015 Asterisk vulnerability and a 2022 Cisco Expressway vulnerability which both had the same number of detections last month and this month, suggesting they are duplicates. Indeed, each vulnerability is caused by a failure to process null-bytes in X.509 certificate CN fields. This is interesting, as while it could indicate that these specific vulnerabilities are being targeted, it could also indicate that another vulnerability involving null-bytes in X.509 certificate CN fields is being targeted or researched. Similarly, there is another two vulnerabilities with identical detection volumes at 7th and 8th place, which show an 1,100% increase in detections. These are a 2009 Windows and 2010 Adobe reader font parsing RCE. Once again, this could indicate targeting of these very old vulnerabilities, or it could indicate targeting and/or research of a new vulnerability. It is always possible however that these detections are not being caused by vulnerability targeting, but are instead just artifacts of some other behavior, such as malformed files being generated through some other process. If that were the case however, it would still beg the question why are they being submitted to VirusTotal.

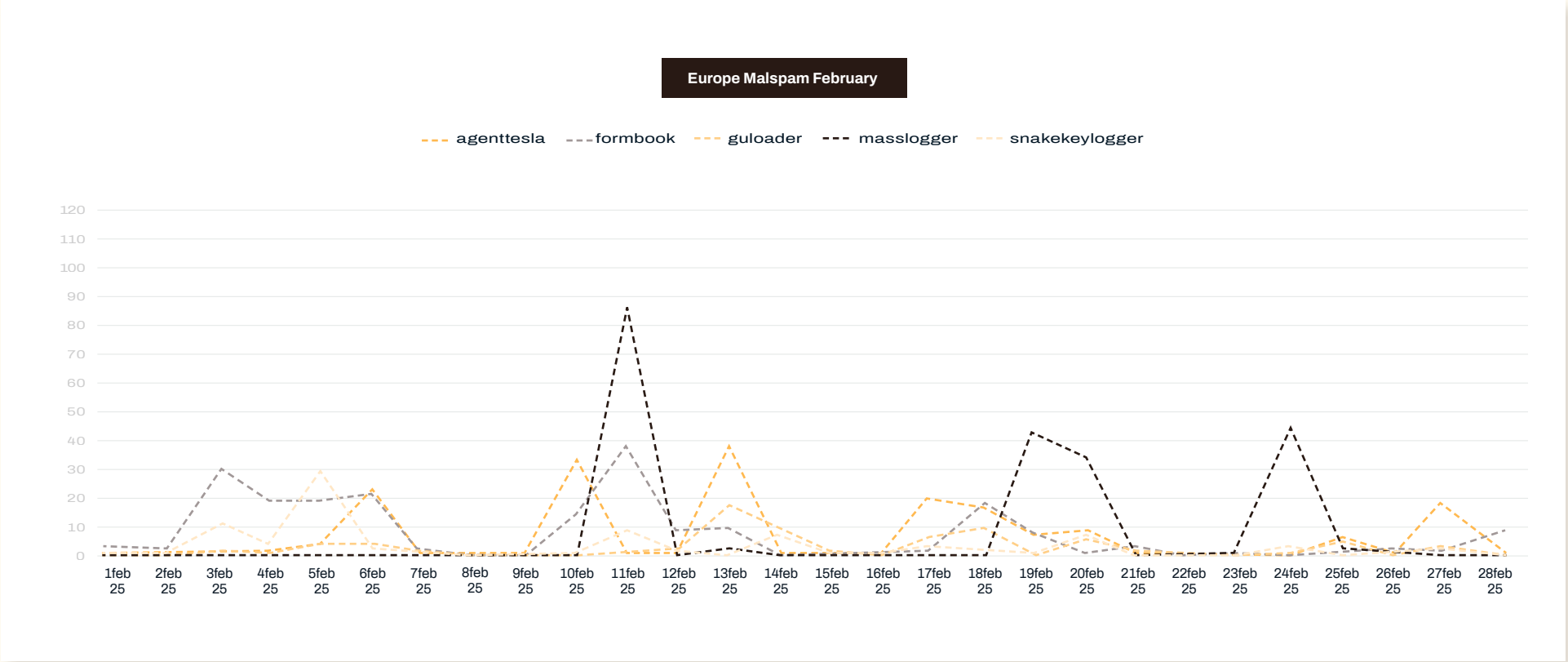
Phishing malware delivery

In the EU Masslogger was the most detected malware family in malspam detections, beating Formbook by a single detection, followed by AgentTesla, Snake Keylogger, and Guloader.

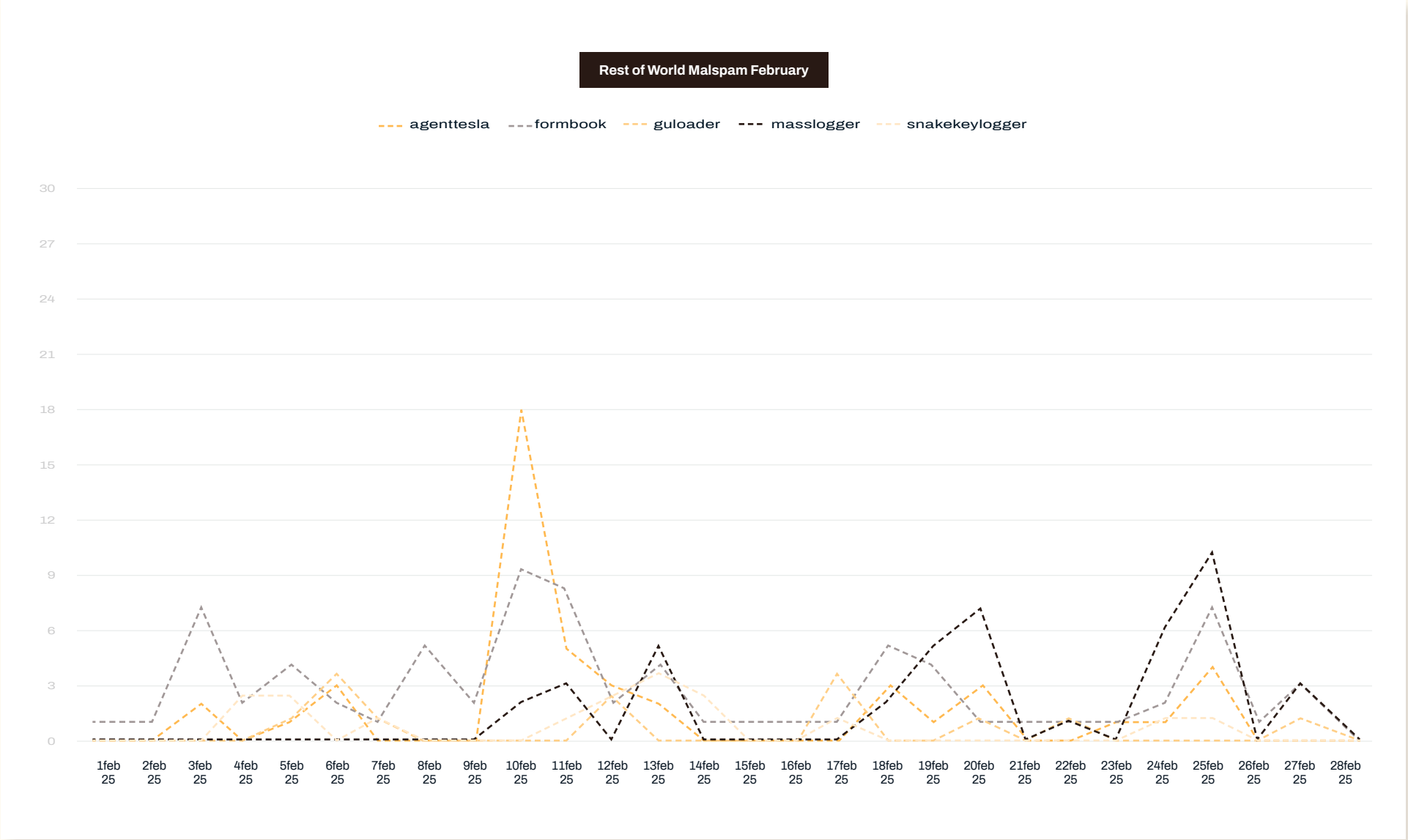
The most commonly detected malware family in malspam for the rest of the world was Formbook, with about 20% more detections than AgentTesla or Masslogger.



Looking at detection volumes over time for Europe, we can see that MassLogger was delivered in several large yet brief spikes, while Formbook was delivered in smaller volumes but more consistently over the month.



In rest of world data, we can see that once again, formbook was delivered more consistently over the month, while AgentTesla and Masslogger instead had several brief spikes in detections.



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.