Monthly Threat Intelligence Rollup

DEEP seas

02/01/25-02/28/25

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
BoltDB Is BunkDB	Researchers at Socket have found a Golang package typosquatting as a well-known database module called BoltDB. This can be considered troublesome because BoltDB is a popular dependency within the Go ecosystem, with around 8,367 other packages utilizing its services. The trojanized instance of BoltDB was noted to contain a backdoor enabling remote code execution. To evade detection, after the malware was cached by the Go Module Mirror, a Git tag was altered on the malware on GitHub to hide traces of malicious intent. At present, this malicious package remains available on the Go Module Proxy and has not been remediated by the Go Module Proxy administrators or GitHub.[i]
Blowing Smoke	Trend Micro's Zero Day Initiative team has observed presumed Russian cyber crime entities attacking Ukrainian organizations through a SmokeLoader malware campaign. To deliver the loader, the malware was spread through spear phishing campaigns that spoofed document extensions using homoglyph attacks to trick victims and Windows into running SmokeLoader. To get the malware to execute successfully, the group used 7-Zip zero-day vulnerability CVE-2025-0411, which permitted circumvention of the Windows Mark-of-the-Web feature by double archiving files, avoiding being flagged and thus avoiding detection. Industries in Ukraine impacted by this campaign include government, manufacturing, public transportation, administration, insurance, pharmaceutical, and public utilities. The CVE mentioned has since been patched by 7-Zip in version 24.09.[ii]
What Goes Around	The private security researcher Raven File recently released details about an ironic event that occurred to the Babuk ransomware group. The ransomware group tied their cryptocurrency wallet to the Indodax Exchange, a crypto trading application for Indonesia. Foreign cryptocurrency exchanges are often utilized by cyber crime actors to launder their ransom payments. However, an unrelated security breach at Indodax occurred, causing the group's funds, along with $20 million, to disappear. Due to the money being acquired through ransoms, it is unlikely that the group will be able to retrieve their stolen cryptocurrency.[iii]
Dirty Money	Symantec's Threat Hunter Team recently linked the Chinese state-aligned espionage group Bronze Starlight (aka Cinnamon Tempest or Emperor Dragonfly) and the actors behind a recent RA World ransomware attack, establishing a hypothesis that Bronze Starlight has begun initiating ransoms for profit, similar to cyber criminal organizations. In both observed incidents the group used a Toshiba executable to sideload a malicious DLL. This DLL acted as a loader and, when executed, searched for and decrypted a DAT file to become the PlugX backdoor, predominantly seen only in Chinese state attacks. The attacker then installed RA World ransomware to the victim's network environment and demanded $2 million for ransom from an unnamed medium-sized software and services company in South Asia. The incident is another piece of evidence of work conducted by Chinese cyber operatives as freelance cyber criminal operators.[iv]

Emergent Malware and TTPs

Newly emerging malware and tactics, techniques, and procedures identified in the last thirty days.

Malware/Campaign	Activity Summary	TTP Analysis
deepseeek, deepseekai	The supply chain security team of the threat intelligence department at the Positive Technologies Expert Security Center uncovered a malicious campaign in the PyPi package repository named “deepseeek” and “deepseekai.”	Upon execution, these packages collect user data, device data, and environment variables. To facilitate command and control communication, the Pipedream platform is used, which is an integration platform used by developers. Notably, these packages were written with the help of an AI assistant, indicating a low level of sophistication from the unknown attacker. This campaign was aimed at developers, ML engineers, and ordinary AI enthusiasts who might be interested in integrating DeepSeek into their systems.[v]
Flesh Stealer Adopts Typical Russian Geofencing Tactics	CYFIRMA has recently examined a stealer known online as “Flesh Stealer.”	Flesh Stealer is a .NET executable written in C# by Russian cyber criminals. It is used to target browsers, including Opera, Chrome, Firefox, and Edge, from which it steals data such as cookies, credentials, and browsing history. The stealer also steals databases and chats from applications such as Signal and Telegram, which is then sent back to the attacker. The malware features anti-debugging, and anti-VM capabilities and is capable of bypassing encryption employed by Chrome. Notably, the malware does not target CIS countries, pointing further towards an eastern European or Russian developer.[vi]
North Korean Operators Integrate RDP Wrapper into their Toolkit	The AhnLab Security Intelligence Center has pointed out the North Korea-based Kimsuky group’s development of a malware variant that allows for remote connections.	The threat group’s new tool is a modified version of RDP Wrapper, an open-source tool that is used for remote desktop purposes. To deliver the malware onto a victim’s device, the Kimsuky actors first deliver a LNK file to the victim through spear-phishing. The file names associated with this activity included both human names and company titles, suggesting that Kimsuky was targeting specific entities. To trick the user into running the malware, the LNK is disguised as a PDF, Excel, or Word document. After the file is executed, PowerShell or Mshta is run to download and execute the RDP Wrapper payload, among other Kimsuky-specific malware.[vii]
LegionLoader Malware on the Rise Among Cyber Criminals	The TEHTRIS threat intelligence team has noticed the increasing trend of a new downloader dubbed “LegionLoader.”	The malware appears to be used by a criminal organization, as the group behind LegionLoader sets their targets globally, with Brazil accounting for around 10% of all victims. The loader is delivered through the venerable drive-by download technique, using insecure websites to redirect users to attacker-controlled domains. After downloading from the malicious website, a user must run the MSI file delivered to them to begin installation. This MSI file contains shellcode that then starts explorer.exe and uses process hollowing to load the next stage of attack using function API calls such as CreateProcessInternalA, ZwQueryInformationProcess, ReadProcessMemory, ZtUnmapViewOfSection, VirtualAllocEx, WriteProcessMemory, and NtResumeThread.[viii]
I2PRAT Representing Another Entry into Cyber Criminal Tool Kits	Sekoia has pointed out a new piece of malware to hit the cyber criminal scene that they have dubbed I2PRAT.	The malware infection chain is described as consisting of three layers, with the first being a commodity packer that executes a loader in memory before executing the second stage. This loader has been seen employing various techniques to elevate its privilege and bypass defenses, such as RPC elevation and parent ID spoofing. This loader then executes the third and final stage of the infection

		chain, the I2PRAT installer. The RAT employs the I2P network to help anonymize its C2 communication. Once a successful C2 connection is established, further commands can be made such as disabling Windows Defender features, bypassing the Windows Filtering Platform, creating auto start services, and more. Based on the DLLs within I2PRAT, the group's targets are clear: files found in File Manager, RDP connections, user accounts, and scheduled tasks for persistence.[ix]
New Post-Exploitation Kit Includes the PATHLOADER, FINALDRAFT Components	Elastic Security Labs has made public a new post-exploitation kit, containing a new loader, backdoor, and submodules.	The loader component, named "PATHLOADER," is an executable file that downloads and executes encrypted shellcode. This shellcode is an implant retrieved from the attacker's C2 which Elastic calls "FINALDRAFT." FINALDRAFT is a C++ backdoor that focuses primarily on data exfiltration and process injection. The backdoor includes additional modules, such as a pass-the-hash module, a PowerPick module, and a network enumeration module, for injection. There are 44 total commands possible with FINALDRAFT, including proxy capabilities, file enumeration, modifying files, modifying running processes, and more.[x]
Unnamed Golang Backdoor Suspected to be of Russian Origin	Netskope Threat Labs' research into a new, currently unnamed backdoor has just been published.	The Golang malware starts its infection chain with the payload first, implementing itself into the "installSelf" function in the main package. If the malware is running in the correct location, the backdoor will begin to use Telegram as its C2 mechanism through an open source Go package. The malware supports four different command options, PowerShell command execution, persistence measures, screenshotting, and self-deletion. Netskope believes the backdoor to be of Russian origin.[xi]
New Vgod Ransomware Making Waves	The CYFIRMA research and advisory team has identified a new ransomware strain which they have named "Vgod Ransomware."	Vgod is a Windows-based ransomware that employs encryption techniques such as encrypting files, defense evasion, and persistence mechanisms. Its method of delivery has so far been seen to be through phishing emails. The ransom note left by the group upon infection states that files are not only encrypted, but that the data was copied and exfiltrated to the attacker prior, which demonstrates a double extortion model. It was also inferred that the group is likely to target both individuals and organizations because they are a criminal organization and not sponsored by a governmental body. Public information regarding this group or malware is limited; however, DeepSeas will continue to follow this group as their tactics, techniques, and procedures become more well-established.[xii]
Snake Keylogger Variant Identified	FortiGuard Labs identified a new variant of the Snake Keylogger in the wild.	The Snake Keylogger variant identified by FortiGuard now uses AutoIt to deliver and execute its payload. This is because the executable is now an AutoIt-compiled binary, increasing the malware's obfuscation and enabling behavior that mimics automation tools. For persistence, the keylogger inserts a VBS script into the Windows startup folder to automate execution upon system reboot. Snake Keylogger also now uses process hollowing for evasion purposes, hiding within the RegSvcs process. Some of the methods Snake Keylogger uses to log victim data include using websites such as checkip[.]dyndns[.]org to retrieve a victim's geolocation and using SetWindowsHookEx API for capturing keystrokes. Other data pursued by the keylogger includes browser autofill systems and credit card details. This stolen information is then sent to the attackers by using SMTP or Telegram bots, along with HTTP post requests for C2 communication.[xiii]
Python-Based XELERA Ransomware Targeting India	Seqrite Labs APT team has published details of a new ransomware strain called "XELERA."	The Python-based ransomware is initially spread through a spear-phishing email, containing a DOC file that holds a secretly embedded OLE object. This OLE object then leads to the installation of XELERA. Important functions of XELERA include terminating processes, monitoring running processes, changing the wallpaper,

		ransom messaging, and more. Further information regarding XELERA is becoming available as research progresses.[xiv]
NailaoLocker A Newly Identified Chinese Ransomware Strain	Orange Cyberdefense's CERT has found evidence regarding a new ransomware strain, named "NailaoLocker" by Orange.	The name comes from the threat actors' name of "Green Nailao," a likely Chinese criminal group. To start infection, the ransomware must first be activated with NailaoLoader. Once installed, NailaoLoader then opens the DAT file where NailaoLocker resides and decrypts the payload. Written in C++, NailaoLocker is technically unimpressive, not guaranteeing full encryption. This is because the ransomware does not check network shares, if any services or processes should be stopped, and if it is being actively debugged. To encrypt files, NailaoLocker appends the "locked" extension and uses asymmetric encryption through AES-256-CTR.[xv]
CashRansomware Potentially a New Offering from Mint Stealer Authors	TEHTRIS has obtained a copy of a novel piece of ransomware called "CashRansomware."	The ransomware is written in C# and lacks the proper obfuscation and encryption you would expect from modern day ransomware. The malware is believed to be developed by those who previously developed Mint Stealer, as CashRansomware was advertised on their Telegram, pointing towards the malware originating from Russia. Defense measures CashRansomware takes include using the Eziriz .NET Reactor tool for obfuscation, geolocation checks, language checks, time-stomping, anti-debugging, anti-sandbox, anti-VM, etc. To run, the ransomware must be executed by the victim, showing a possible social engineering aspect to initial infection. After infection, CashRansomware will wreak havoc by modifying system files, disabling security measures, and fully encrypting the victim's data.[xvi]

Threat Actor Campaigns

New activity related to threat actor campaigns in the last thirty days.

Threat Actors	Activity Summary
XE Group Targeting Supply Chain Vendors	Intezer has been tracking recent changes made to the attack methodology of the cyber criminal threat group, XE Group. These changes include now targeting supply chain vendors in the manufacturing and distribution sectors, their use of evolved custom ASPXSPY webshells, and using new zero-day vulnerabilities for initial access. These webshells use zero-days, such as CVE-2024-57968 and CVE-2025-25181, to gain access through successful SQL injection attacks targeting the VeraCore application IIS server hosting VeraCore's warehouse management system software. By doing so, the attackers are able to retrieve user credentials, which are then used to exploit the upload feature within the VeraCore application. Using this feature, the attackers are able to upload further webshells onto the victim's device.[xvii]
APT44 Linked to BACKORDER Loader Malware	EclecticIQ analysts have identified modifications made by Russia's APT44 to a loader, which they call "BACKORDER." This loader is delivered through ZIP files disguised as KMS activation tools hosted on Torrent websites or typosquatting domains. Upon opening BACKORDER, the victim is greeted with a GUI for KMS activation to deceive them while the loader runs in the background. Some of BACKORDER's unique features include disabling Microsoft Defender, preventing Windows Updates, using scheduled tasks to establish persistence, and adding exclusion rules pertaining to particular directories. BACKORDER's main purpose, however, is the installation of DcRAT to exfiltrate sensitive data.[xviii]
Winnti Group Exploiting ERP Systems to Drop Webshells	LAC's Cyber Emergency Center has made light of a new campaign from the Chinese Winnti Group titled "RevivalStone." The infection chain of this campaign begins with the Winnti Group exploiting ERP systems on a victim's web server with SQL injection vulnerabilities to install a webshell. The webshell is then used to do reconnaissance and credential theft for lateral movement purposes. Winnti malware is then placed on the victim's affected devices. The group then used these credentials to perform a supply chain attack against the victim's collaborative organizations. Victimology for this campaign was solely focused on Japanese companies in the manufacturing, materials, and energy sectors.[xix]
APT44's BadPilot Campaign Targeting Western Nations	Microsoft Threat Intelligence has tracked down a subsection of the Russian threat actor, APT44, not previously discussed online. This subsection called the "BadPilot campaign" is known for targeting critical industries such as energy, oil and gas, telecommunications, shipping, arms manufacturing, and government. The group is currently targeting the United States, Canada, Australia, and the United Kingdom, but has also targeted others, including Ukraine and countries in Europe, Central Asia, and the Middle East. Typically, for initial access, the group will exploit vulnerable Microsoft Exchange Internet-facing devices through tools such as Shodan, third-party internet scanning services, and knowledge repositories. Once exploited, the group downloads webshells for persistence, performs lateral movement techniques, and eventually deploys more malware.[xx]
DeceptiveDevelopment Campaign Targeting Cryptocurrency with BeaverTail, InvisibleFerret Malwares	ESET researchers broke down a new campaign that they have designated as "DeceptiveDevelopment," a North Korean threat group that primarily steals cryptocurrency for financial gain with hints of potential espionage activities. The group targets software developers on all OS platforms, initiating access with them through phony job opportunities posted online, where the victim is convinced to download various malware for the interview process. The malware DeceptiveDevelopment installs on the victim's device usually starts with BeaverTail infostealer, which then downloads an InvisibleFerret loader. InvisibleFerret then installs further modules for itself to enhance its capabilities. Finally, a copy of AnyDesk is installed, allowing remote access for the attackers. This activity is similar to that seen in other North Korean campaigns such as Moonstone Sleet, Lazarus's DreamJob, and DangerousPassword.[xxi]
Cl0p Ransomware Group Accelerating Operations	The Cyberint Research Team has tracked the Cl0p ransomware gang for some time now and has found new evidence showing a revival in the group after a scaling down their attacks in 2024 compared to 2023. Recently, however, Cl0p has been seen on the

	move again, targeting organizations with CVE-2024-50623, a vulnerability in Cleo products such as Cleo LexiCom, Cleo VLTrader, and Cleo Harmony, that allows for unrestricted file uploads and downloads, leading to remote code execution. This has since been patched, but that did not matter to Cl0p, who already had 66 companies' data before it was patched. The group often will reach out directly to the victim for payment through secure chatrooms and email. In February, there were about 80 attacks, demonstrating the group's return.[xxii]

Dark Web Markets

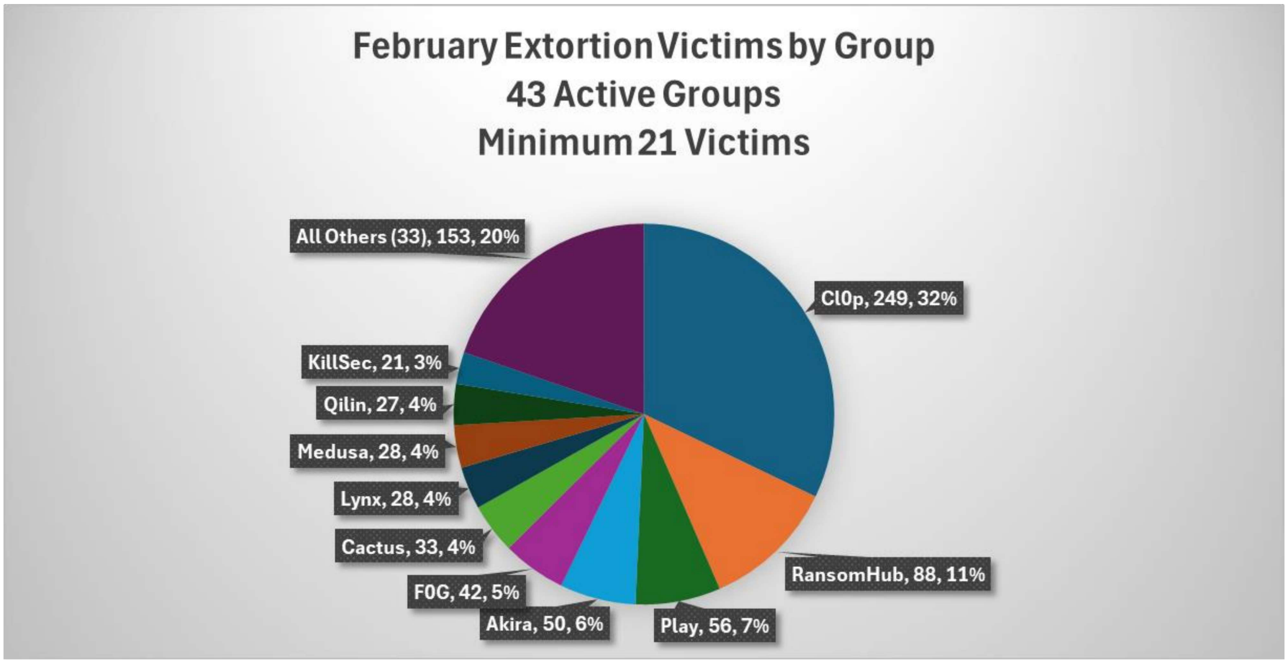
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

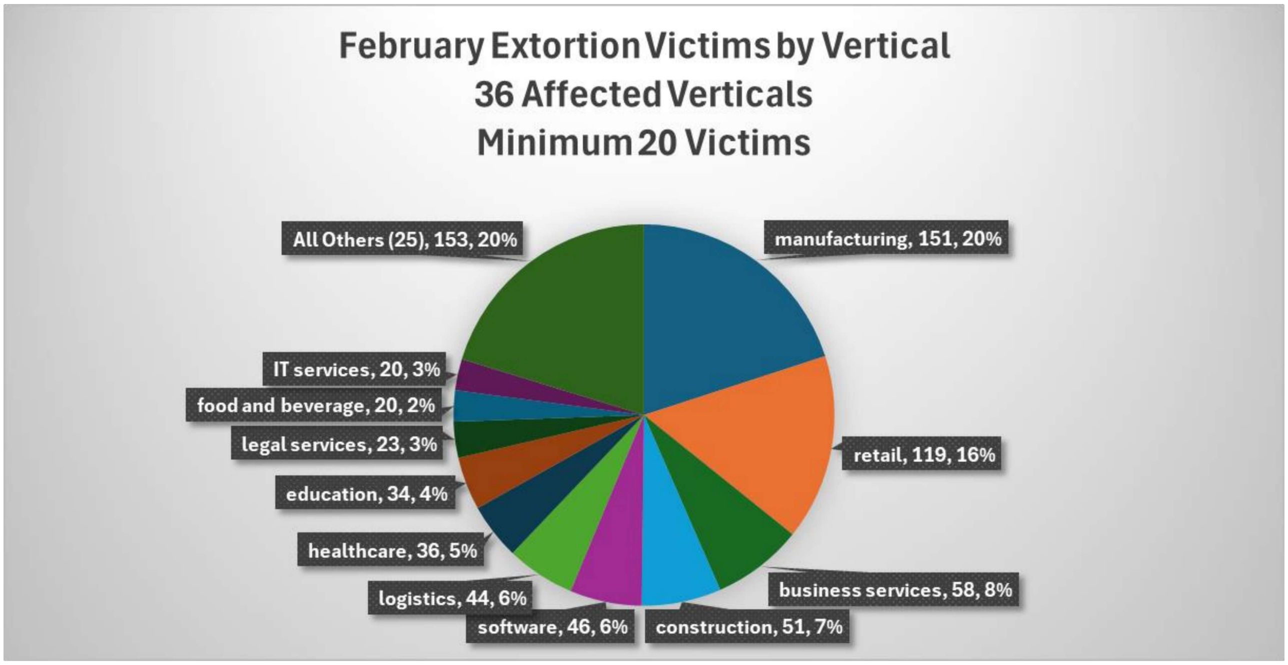
Activity	Note
Actor Developments	A multinational law enforcement operation resulted in the shutdown of two prominent cybercrime forums, Nulled[.]io and Cracked[.]io. This is not expected to significantly impact the sale of stolen credentials and malware, as actors on these two forums participate in multiple forums, as well as in public and private chats on platforms such as Telegram and Discord.
Tool Sale	A relatively new crime forum actor was observed selling extended validation GlobalSign code signing certificates for USD 3,500 - which is significantly ($500-$1,500) cheaper than other actors selling similar products. He is likely credible as he has one successful transaction using the automated escrow system.
Access Sale	An actor connected with a ransomware extortion team advertised the sale of an unidentified U.S. based cyber threat intelligence company with around USD 800 million in revenue for USD 1000.
Access Sale	An actor was observed selling RMM agent local admin access to an unnamed U.S. based hospitality company with more than USD 230 million in revenue. He did not name a price.
Access Sale	An actor was observed selling local admin access to an unnamed U.S. based logistics company with USD 196 million in revenue. He did not name a price.
Access Sale	An actor was observed selling RDweb local user access to a U.S. based "crypto" company with USD 631 million in revenue for a percentage of the revenue realized by exploiting it. There are 50,030 hosts on the network and 26 domain controllers.
Tool Sale	A veteran criminal forum actor relaunched a new version of his Data Fusion shop in which he claims he has a database of 300 million fullz (name, SSN, address, telephone, and other data), which if true would be most Americans. He claims to generate his own background reports and has a marketplace for other actors to sell their own digital goods.
Access Sale	An access seller was observed selling domain admin access to a Pakistan based pharmaceutical company with USD 518 million in revenue for USD 6,000.
Access Sale	An access seller was observed selling Fortinet domain user access to a U.S. based CRM software company with USD 3 billion in revenue for USD 1,200.
Access Sale	An access seller was observed selling RDP user access to a UK based company in an unnamed vertical with USD 1.7 billion in revenue.
Access Sale	An access seller was observed selling access to multiple U.S. based victims, including a business services company with USD 28.8 million in revenue for USD 1,400 and a company in the energy, utilities, and waste vertical with USD 7.3 million in revenue and 323 employees for USD 700.
Actor Developments	Chat logs belonging to the Black Basta ransomware gang were leaked, supposedly in retaliation for Black Basta attacks against Russian banks. The chats revealed not only tactics, techniques, and procedures used by the group; they also revealed significant operational difficulties caused by personality conflicts in the group. There has been no activity on the Black Basta victim disclosure site since mid-January, and, reportedly, some members of the group have already left and joined other ransomware groups.
Access Sale	An access seller was observed selling Fortinet VPN access to 84 devices on a network belonging to a U.S. based manufacturing company with USD 1 billion in revenue. When asked by a big game hunting ransomware operator why there were so few devices, the seller responded that the access was to a Windows 7 share folder and the access was VPN only, and not RDP.

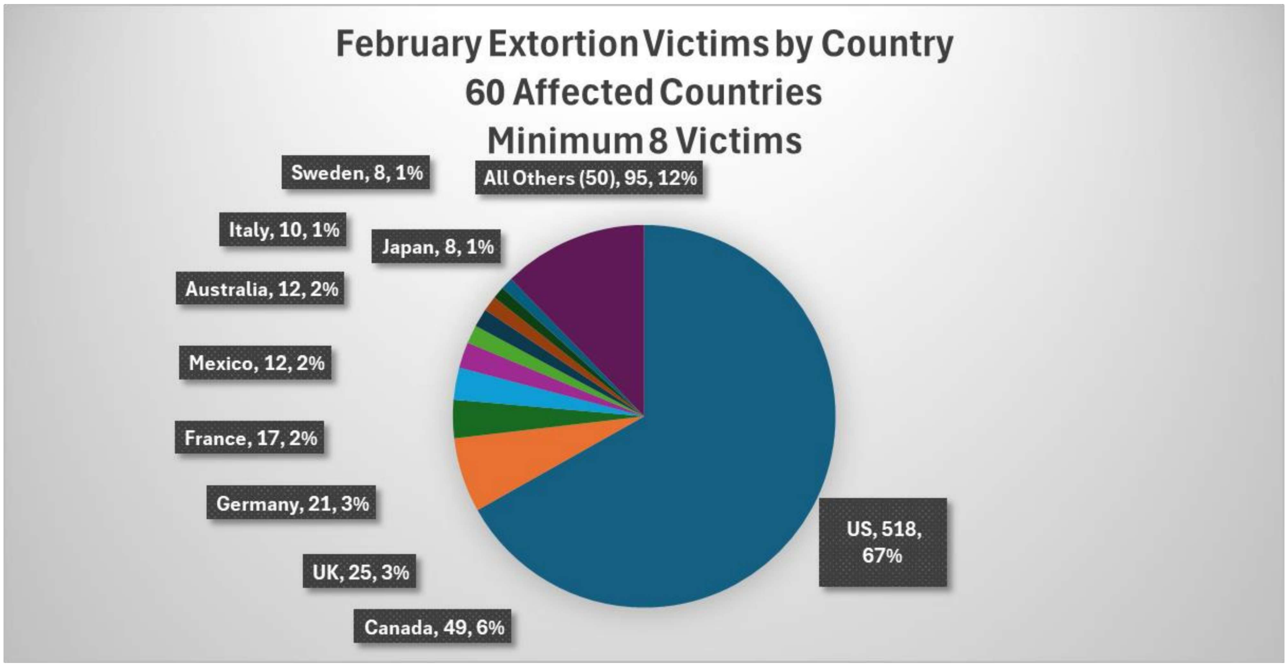
Access Sale	An access seller was observed selling an RCE on a network belonging to a U.S. based holding company with USD 2.6 billion in revenue. He did not specify the vulnerability exploited.
Access Sale	An access seller was observed selling RDP user access to an unnamed U.S. based law firm with around USD 400 million in revenue for USD 1,000. Another user offered USD 200 complaining there wasn't enough information to properly evaluate the price.
Access Sale	An access seller was observed selling an RCE in a network belonging to an unnamed Japan based food company with USD 12 billion in revenue.

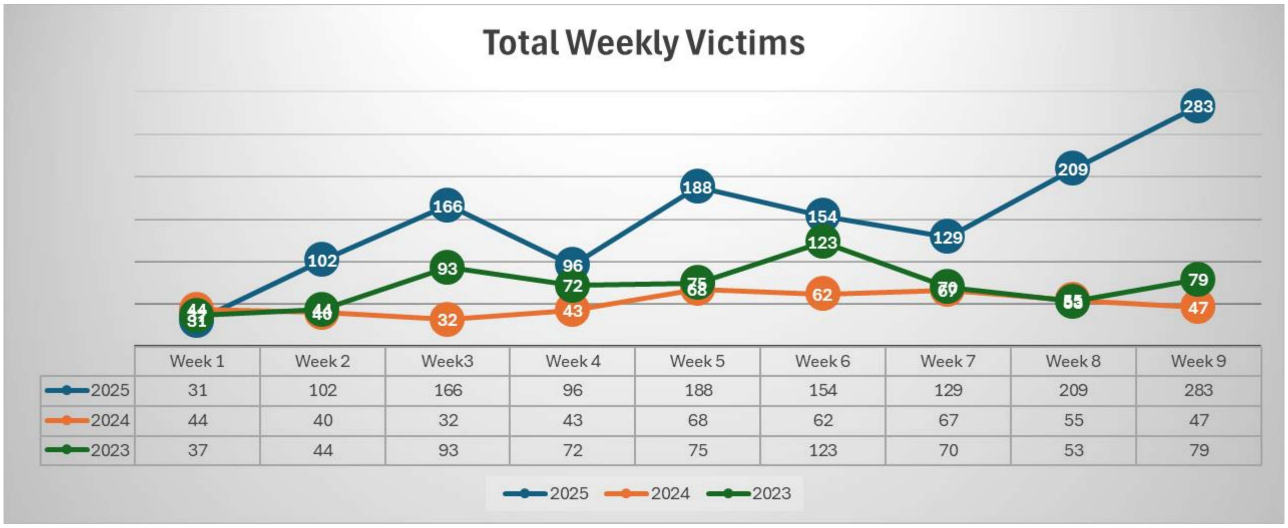
By The Numbers

Summarizing incidents in graphical format

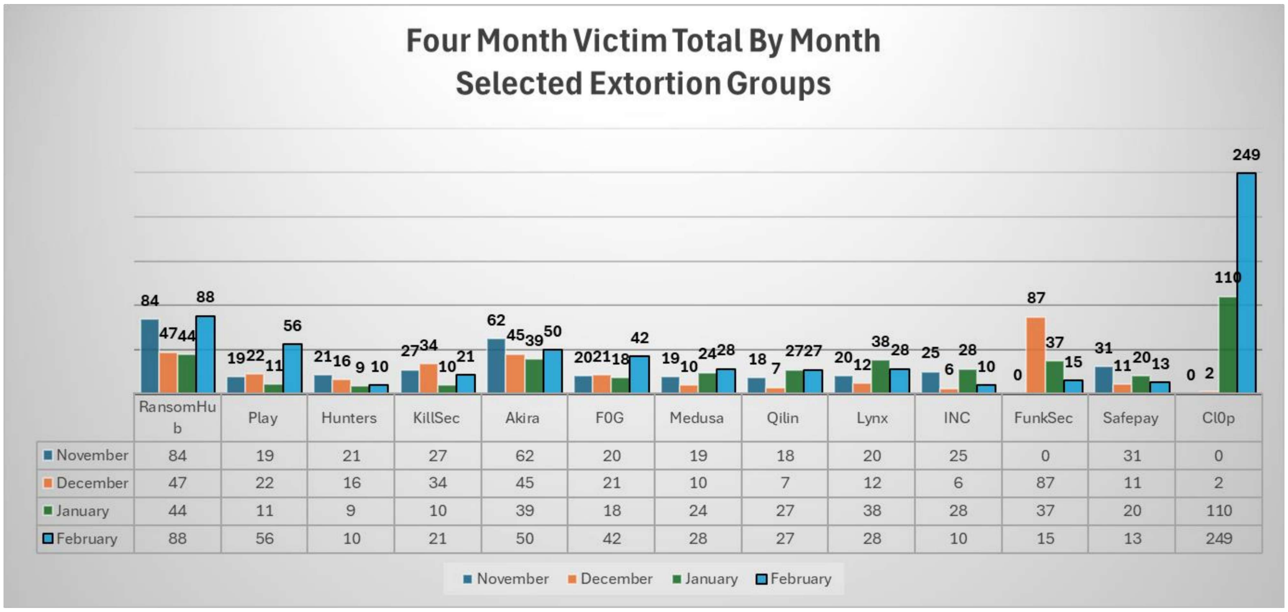








	Week 1	Week 2	Week3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9
2025	31	102	166	96	188	154	129	209	283
2024	44	40	32	43	68	62	67	55	47
2023	37	44	93	72	75	123	70	53	79



Four Month Victim Total By Month
Selected Extortion Groups

	RansomHub	Play	Hunters	KillSec	Akira	F0G	Medusa	Qilin	Lynx	INC	FunkSec	Safepay	Cl0p
■ November	84	19	21	27	62	20	19	18	20	25	0	31	0
■ December	47	22	16	34	45	21	10	7	12	6	87	11	2
■ January	44	11	9	10	39	18	24	27	38	28	37	20	110
□ February	88	56	10	21	50	42	28	27	28	10	15	13	249

New Detection Content

Noteworthy or unique detection logic added in the last 30 days, excluding rule tuning. Not all rules or platforms are represented in this list (e.g., Azure Sentinel, Corelight, etc.)

- **Defense Evasion - AuditPol Disabling Logging Policies Detected – Modified**
  - This is a modified version of the Carbon Black detection to tune out false positives. Their description: "This query looks for usage of auditpol to disable event logging for category or subcategory policies. Threat: An adversary may choose to clean up their tracks by disabling event logging for certain suspicious activities. Auditpol is a tool native to Windows machines. Therefore, attackers do not need to drop additional files; instead, they can use this executable to prevent collection of audit logs and additional evidence. False Positives: Though not very common, other IT software and administrative tools may leverage auditpol commands."
  - **Platforms:** Carbon Black, CrowdStrike, Defender

[i] https://socket.dev/blog/malicious-package-exploits-go-module-proxy-caching-for-persistence

[ii] https://trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html

[iii] https://theravenfile.com/2025/02/06/babuk-ransomware-a-victim-of-indodax-hack

[iv] https://security.com/threat-intelligence/chinese-espionage-ransomware

[v] https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/malicious-packages-deepseeek-and-deepseekai-published-in-python-package-index

[vi] https://cyfirma.com/research/flesh-stealer-unmasking-the-blue-masked-thief

[vii] https://asec.ahnlab.com/en/86098

[viii] https://tehtris.com/en/blog/legionloader-exposed

[ix] https://blog.sekoia.io/ratatouille-cooking-up-chaos-in-the-i2p-kitchen

[x] https://elastic.co/security-labs/finaldraft

[xi] https://netskope.com/blog/telegram-abused-as-c2-channel-for-new-golang-backdoor

[xii] https://cyfirma.com/research/vgod-ransomware

[xiii] https://fortinet.com/blog/threat-research/fortisandbox-detects-evolving-snake-keylogger-variant

[xiv] https://seqrite.com/blog/xelera-ransomware-fake-fci-job-offers

[xv] https://orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

[xvi] https://tehtris.com/en/blog/unreleased-raas-analysis-cashransomware

[xvii] https://intezer.com/blog/research/xe-group-exploiting-zero-days

[xviii] https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns

[xix] https://lac.co.jp/lacwatch/report/20250213_004283.html

[xx] https://microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation

[xxi] https://welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers

[xxii] https://cyberint.com/blog/dark-web/cl0p-ransomware