Monthly Threat Intelligence Rollup

DEEP seas

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Fooling the Industry's Best	The ThreatBook Research and Response Team has caught up with the recent activity of the Southeast Asian APT threat group, APT32, also known as OceanLotus. In their newest campaign, the group used GitHub poisoning to backdoor a red team tool hosted on GitHub and used for privilege escalation. APT32 will even build out fake GitHub profiles for the accounts hosting the malware on GitHub, making it appear more legitimate. To deliver the malware, APT32 embeds a malicious .suo file into a Visual Studio project, which executes a trojan that then reaches out to download the GitHub payload. According to ThreatBook, this campaign has greatly affected the cybersecurity industry in China, with many Chinese cybersecurity researchers reporting remote control or data theft attempts.[i]
Another KO on Ivanti's Record	This month, the FortiGuard Incident Response (FGIR) team revealed a new rootkit named "sysinitd.ko." To establish an initial foothold on a potential victim's device, the threat actor first exploited three Ivanti Cloud Services Appliance vulnerabilities, CVE-2024-8190, CVE-2024-8963, and CVE-2024-9380. The rootkit is delivered by an injector script labelled "install.sh" that installs the malicious kernel module shareable object, "sysinitd.so" (the sysinitd.ko rootkit), to the file directory /usr/share/empty. This kernel module then sets a Netfilter hook function on NF_INET_PRE_ROUTING to take control of any incoming TCP traffic to the victim device. To establish persistence, sysinitd.ko added entries to the /etc/rc.local and /etc/rc.d/rc.local files so the rootkit malware is loaded during system startup.[ii]
Kitty Sharpens Its Claws	QiAnXin XLab has tracked the updated AISURU botnet to its newest rendition, "kitty." Kitty is considered a newer version of AISURU due to improvements such as using socks5 proxies for C2 communication, with 250 proxies and 55 C2s seen being used. The main purpose for the botnet is DDoS, with additional reverse shell functions. Possible commands include starting a reverse shell, starting and stopping DDoS attacks, and aborting. Besides these new features, similar features from AISURU still exist, including exploiting 0day vulnerabilities in cnPilot routers for initial access. The latest sighting of this botnet was the recent large-scale DDoS attack on the digital distribution platform Steam and the Perfect World Esports Platform.[iii]
Not a Nominal Attack	ISPreview received news from the UK internet domain registry Nominet stating that the Ivanti VPN the company used suffered from a 0day vulnerability and fell victim to an intrusion allowing for unauthorized remote access. The vulnerabilities, CVE-2025-0282 and CVE-2025-0283, are known to infect Ivanti Connect Secure, Policy Secure, and ZTA Gateways. Nominet stated that no data was exfiltrated and no further backdoors or artifacts of the attack were present as well. Due to the potential effects of such an attack, and given Nominet manages over 11 million .uk domain names, the hope of there being no further compromise is strong.[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
PLAYFULGHOST Not Playing Around	On the Google Cloud Security Community blog from Mandiant Managed Defense is a novel backdoor called “PLAYFULGHOST” due to its similarities with the well-established Gh0st RAT.	For initial delivery, the actor behind PLAYFULGHOST utilizes phishing or SEO poisoning to lure victims. After installation, the malware’s execution is done in three parts: a legitimate executable that is vulnerable to DLL search order hijacking, a malicious DLL file that functions as a launcher in the same folder as the legitimate executable, and the PLAYFULGHOST payload. These files are interchangeable, allowing for multiple methods of executing the backdoor. The simplest method is that the threat actor renames a copy of a legitimate signed executable from Tencent to "svchost.exe" and uses it to load a malicious launcher DLL, which then decrypts and loads PLAYFULGHOST into memory. PLAYFULGHOST can also perform a plethora of actions such as keylogging, screen capture, audio capture, remote shell, file transfer, file execution, and much more.[v]
Nothing Normal about This One	CYFIRMA recently presented the public with their findings on a new remote access trojan titled “NonEuclid.”	The RAT functions on C# and is built for version 4.8 of the .NET framework. It also features a large assortment of capabilities, including privilege escalation, dynamic DLL loading, configuring settings, AES encryption to encrypt key target files, logging, and more. For defense evasion alone, NonEuclid can delay startup, usurp critical process handling, perform anti-AV or VM scans, validate administrative privileges, ensure there are no duplicates, and secure socket C2 communication. The RAT is being sold over cybercriminal online forums and has likely been developed by criminals in Russia for financial gain.[vi]
A Hard Pill to Swallow	Cyjax has uncovered a new data-leak site (DLS) for a previously unknown extortion group “Morpheus.”	So far, the group has only impacted two organizations in the pharmaceutical and manufacturing industries in Australia and Germany. Security researchers have said that the group uses ransomware such as Hellcat, which uses identical code for their ransomware payloads. Due to their absence on cybercriminal forums, social media platforms, and Telegram, Morpheus seems to be confined to its DLS for interaction with their clients. The group seeks out both PII and confidential information to use against its victims.[vii]
FastPass to Unauthorized Access	SpearTip has found a new exploit centered around the Fasthttp HTTP server and client library.	This exploit allows for unauthorized access to accounts through spamming brute-force login attempts and MFA requests. Initial access seems to be done through the Azure Active Directory Graph API. While around 65% of recorded incidents using Fasthttp in this manner were from Brazil, a definitive answer on where the attacks may be originating from has not yet been made. The first recorded use of Fasthttp was on January 6, 2025.[viii]
Mirai? No… Murdoc!	The Qualys Threat Research Unit has unearthed a new variant of Mirai, which Qualys has dubbed “Murdoc Botnet.”	The malware targets vulnerabilities within AVTECH cameras and Huawei HG532 routers, such as CVE-2024-7029 and CVE-2017-17215, for initial access. The threat actors behind this botnet appear to have a lot of support, as they have over 100 servers to communicate with affected devices and over 1,300 IPs were found connected to the campaign. Murdoc

		Botnet’s top targets include entities in Malaysia, Thailand, Mexico, and Indonesia.[ix]
A Minty Fresh Loader	Broadcom has put out a bulletin this month letting the public know about a new loader making its rounds online, called “MintsLoader.”	This malware begins infection through malicious links in phishing emails sent by threat actors. The links within the emails facilitate the download of malicious Jscript files, which infect the victim with further malware, such as StealC or the BOINC client. The attacker’s goal is to exfiltrate data from victims’ web browsers, applications, and crypto wallets to their C2 server. Impacted sectors include electricity, gas and oil, law firms, and legal service industries within the U.S. and Europe.[x]
New Xloader Versions Six & Seven	Zscaler ThreatLabz recently posted their findings regarding the newest variants of Xloader, versions six and seven.	These versions update Xloader by adding additional obfuscation and encryption layers to protect Xloader from signature-based detection and resist reverse engineering efforts. Xloader now uses “NOPUSHEBP” and “PUSHEBP” as encryption functions and decrypts itself using functions in order from one to three. These functions can perform other actions, such as persistence, C2 communication, and more. Notably, there are no hardcoded keys since the malware is now constructed dynamically. Xloader has also introduced techniques that were previously observed in malware, such as SmokeLoader, which encrypts parts of code at runtime and implements NTDLL hook evasion.[xi]
ScatterBrain Is More Put Together than it Lets On	The Google Threat Intelligence Group posted its research regarding “ScatterBrain,” an obfuscator that has been seen used by Chinese sponsored threat groups with targets in the Europe and the Asia Pacific region.	ScatterBrain has three “protection” modes: “selective” - only obfuscating specified functions, “complete” - obfuscating all functions, and “complete headerless” - which is similar to complete but removes the PE header. Some components previously mentioned that ScatterBrain uses include selective or full control flow graph obfuscation - which restructures a program’s control flow, instruction mutations - used to obscure functionality, and complete import protection - entirely protecting the malware’s import table from analysis. The malware also uses techniques, such as implementing frivolous opaque predicates, which appear straightforward to analysts but confuse binary analysis frameworks.[xii]
Aquabot Upgrades Mirai Source Code Yet Again	The Akamai Security Intelligence and Response Team has noticed changes made to Mirai-based malware, Aquabot, changing its name to “Aquabotv3.”	The new features of Aquabotv3 include the exploitation of the command injection vulnerability (CVE-2024-41710) against Mitel 6800, 6900, and 6900w series SIP phones. The malware now also can actively scan networks for devices vulnerable to exploits, such as discovering new targets for DDoS purposes. Aquabotv3 has been seen carrying new malware payloads as well, allowing for new malware to be dropped. The threat actor behind Aquabot also has improved the botnet, leveraging a more sophisticated C2 infrastructure for better control and evasion detection. Speaking of evasion detection, the malware features improved methods to avoid detection from firewalls, sandboxing, and intrusion detection systems.[xiii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
EAGER for Infection	Kaspersky has documented changes made to the EAGERBEE backdoor, specifically with the employment of new components and plugins used to initiate infection and to further EAGERBEE's malicious capabilities. The first component, the service injector, works by targeting the Windows Themes service process and injects the EAGERBEE backdoor into it. The other component, the plugin orchestrator, is used to interact and manipulate later installed plugins, along with collecting system data and C2 communication. In total, there are five plugins: the File Manager plugin, the Process Manager plugin, the Remote Access Manager plugin, the Service Manager plugin, and the Network Manager plugin. Each of these plugins interact with what they are named, the File Manager plugin works with the File Manager and so on. These plugins can not only retrieve system information but can also perform actions such as process injection, terminating processes, starting malicious RDP sessions, and more. This malware was attributed to the unnamed China-based threat group behind the CoughingDown backdoor.[xiv]
Too Good to be True	The FACCT Threat Intelligence Department has investigated and identified a new threat group going by "FakeTicketer." The name was given because the first attack discovered used Russian Premier League soccer match tickets as decoy documents. The main goal of the group appears to be espionage, targeting government officials and sports officials. The group has been seen deploying multiple pieces of novel malware to their victims named "Zagrebator.Dropper," "Zagrebator.Stealer," or "Zagrebator.RAT" by FACCT. All of these tools are used to facilitate data theft from browsers. Zagrebator.RAT's remote command options include saving content to a specified file, detect and exfiltrate data to the attacker's C2, delete files, and reboot the affected system.[xv]
Watch as your Data… Disappears!	The Black Lotus Labs team at Lumen Technologies has identified a new campaign they labelled "J-magic," which has been performing backdoor-like attacks against Juniper routers and VPN gateways. The name J-magic comes from its file name "JunoscriptService," which is named to appear as a legitimate Junos automation scripting service. After installation, J-magic will start a passive pcap listening process set to observe all inbound TCP traffic, filtering for a specific condition established by the threat actor. This includes various specific byte offsets of certain sizes and at certain locations, checking that traffic is coming to and from threat actor-controlled IPs, and port validation. If these results match what is expected, a reverse shell is spun up. Following infection by J-magic, the threat actors install malware such as a custom variant of cd00r.[xvi]
Silent Lynx Stalking Its Prey	The Seqrite Labs APT-Team released their findings on a new threat group they call "Silent Lynx." The group initiates interaction with the victim through a phishing email that contains a RAR file. In one Silent Lynx campaign, this RAR file contained an ISO file, which holds a decoy PDF file and a C++ loader executable that spawns a PowerShell process to communicate back with Silent Lynx. The other campaign featured another decoy PDF file, along with a Golang executable disguised as a Word document. This fake Word document is a reverse shell, allowing for C2 communication. Previous targets for this group include embassies, lawyers, government banks, and government think-tanks in Kyrgyzstan and Turkmenistan.[xvii]
Demons in the Distance	ESET researchers have made connections between the backdoor SlowStepper and its new associated threat group, named "PlushDaemon" by ESET. The attack happens when a victim downloads the IPany VPN that has been trojanized by PlushDaemon. To start infection, a loader called "AutoMsg.dll" is run, which later allows SlowStepper to function. This backdoor contains more than 30 components, which allow the malware to perform actions such as collecting and exfiltrating data, executing modules, deleting

	files, uninstalling itself, terminating processes, and more. This China-based threat group performs espionage for the country and so far, has been seen targeting a South Korean VPN company.[xviii]
New Extortion Group Makes Headlines	Cyjax has taken notice of a new extortion group calling themselves “GD LockerSec.” The group’s members are from around the globe and are solely financially motivated. They have stated on their DLS that they refuse to victimize a company if they consider it morally wrong. For example, they may not victimize non-profits. Along with their DLS, the group has been seen on BreachForums selling stolen data. Victim countries claiming to be targeted by GD LockerSec include China, Nigeria, and Morocco, with targeted industries being manufacturing, governmental organizations, universities, and cloud computing platforms such as AWS.[xix]
You’ve Heard of SkyNet…	Cisco Talos has brought to light a new campaign by an unknown financially motivated threat actor targeting Poland and Germany. This threat actor was seen pushing a previously undocumented backdoor that Cisco Talos has designated as “TorNet.” As with many recent campaigns, the attack begins with a phishing email with a malicious TGZ file attached. This file contains a .NET loader that decrypts and runs PureCrypter reflectively, which later leads to dropping and execution of TorNet. The backdoor can then communicate with its C2 securely, leveraging the TOR network to anonymize the connection and evade detection.[xx]
Russian Espionage Continues	Bitdefender Labs has warned the public about a new threat group tracked as “UAC-0063” by CERT-UA, which has been running espionage campaigns against organizations in Central Asia and European countries, including government entities and diplomatic missions. The group has had previous connections to APT28, establishing itself as a tool for the Russian government. For initial access, the group weaponizes Microsoft Word documents to deliver the HATVIBE loader. Another tool, “DownExPyer,” is used to maintain persistence and issue commands to the affected machine. These include options such as preparing data for exfiltration, deleting files, executing commands, scanning files, screenshotting, and terminating tasks. The data collected is then exfiltrated through a USB data exfiltrator that Bitdefender calls “PyPlunderPlug.”[xxi]

Dark Web Markets

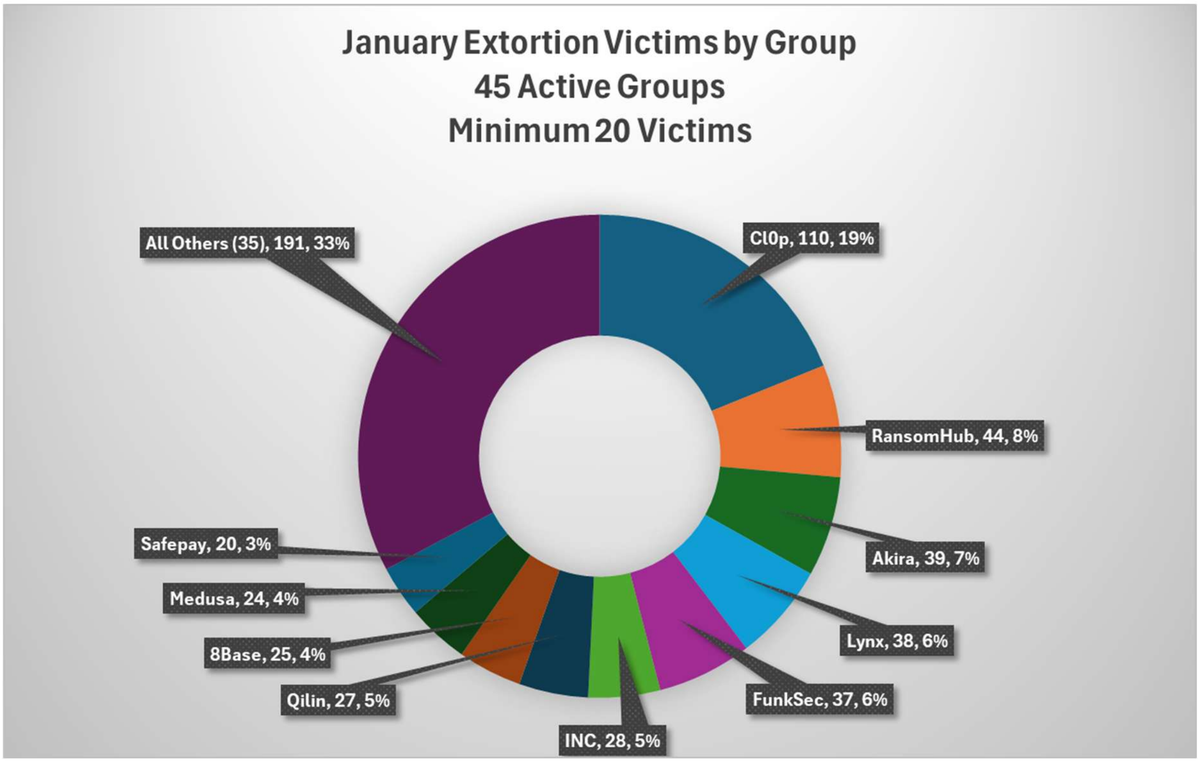
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

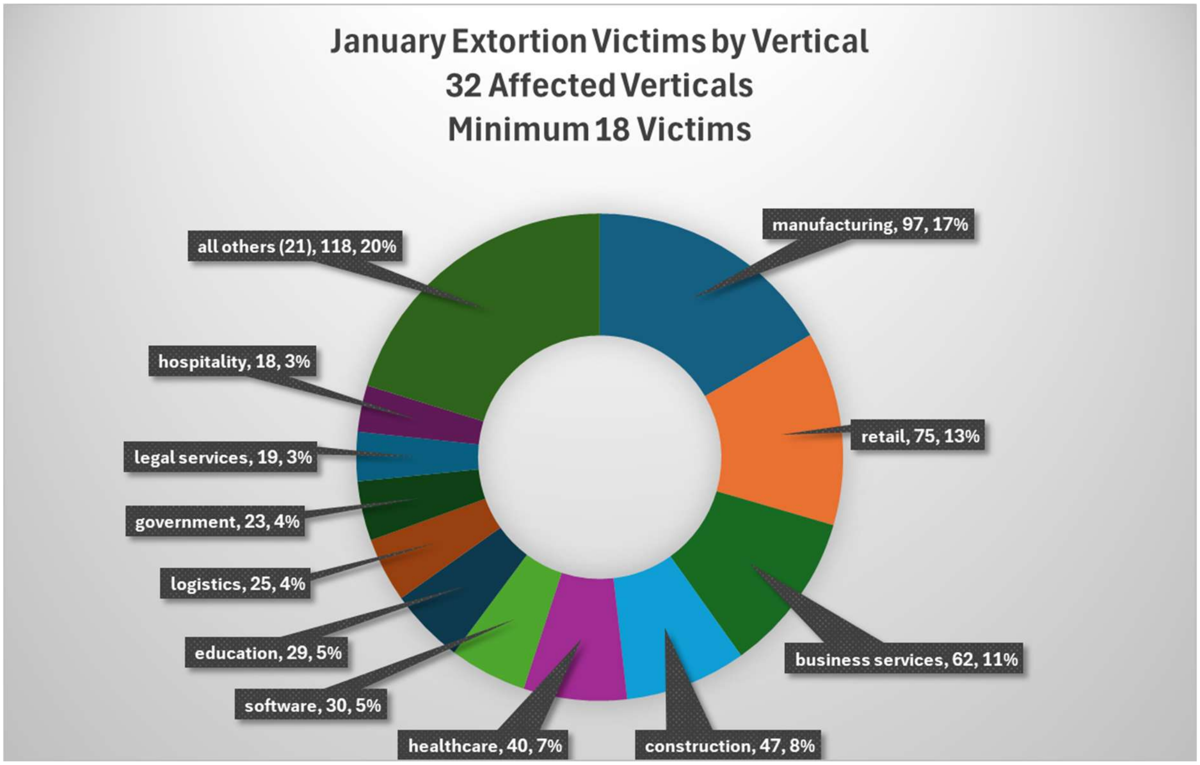
Activity	Note
Access Sale	An actor on a popular criminal forum was selling domain admin access to a U.S. based transportation enterprise with USD 270 million in revenue for a buy now price of USD 20,000.
Tool Sale	An actor on a popular criminal forum was selling what he claimed was a preauth RCE 0day in Cisco WebUI 17.9.4 and earlier. He did not name a price or further elaborate on the RCE.
Tool Sale	An actor on a popular criminal forum was selling what he claimed were multiple preauth RCE 0days in multiple devices: • A preauth RCE Cisco WebUI 17.9.4 and earlier • A preauth RCE 0Day affecting 74,394 Linksys lrt224 routers • A preauth RCE affecting SonicWall VPNs through version 10.x • A preauth RCE 0ay in Sonicwall SRA 4600 version 9.0.0.5-19sv • Another Exploit crime forum actor and known ransomware actor bought supposed Sonic Wall 0 Day for USD 50,000 and found that it only worked on version 9 rather all versions through 10 as advertised. He did not further describe the vulnerabilities or name a price.
Access Sale	An access seller on a popular criminal forum was observed selling multiple illicit accesses: • RDWeb access to a U.S. based software company with USD 29.3 million in revenue and 123 employees for USD 2,000 • Domain user Fortinet VPN access to a U.S. based furniture retailer with USD 21.8 million in revenue for USD 1,500 • Domain user Palo Alto VPN access to a Sweden based automotive service and collision repair enterprise with USD 128.9 million in revenue for USD 1,300. • Domain user Palo Alto VPN access to a Germany based grocery retail enterprise with USD 689.6 million in revenue and 2022 employees for USD 1,600 • Domain user RDweb access to a U.S. based sporting and recreational equipment retailer with USD 59.4 million in revenue and 97 employees for USD 1,500
Access Sale	An actor on a popular English language crime forum was selling RDP domain user access to a U.S. based electronics enterprise with USD 1.3 billion in revenue for USD 1,000.
Access Sale	An actor on a Russian language crime forum was selling RDP domain access to a U.S. based general education enterprise with USD 110 million in revenue for USD 2,000.
Data Sale	A reputable long-time user on a Russian language crime forum claimed that he had access to 6.9 TB of information stolen from data analytics firm Gravy Analytics and will expose "the juiciest parts" if Gravy does not comply with his demands. He provided 1 GB of data to prove access, which researchers used to show precise locations of phones belonging to people who have downloaded apps of Gravy Analytics clients.
Access Sale	An access seller on a popular criminal forum was selling ERP database access to a U.S. manufacturer of hearing aids with between USD 500-600 million in revenue for a starting bid of USD 250. Information included access to 683,000 lines of patient data, 1.9 million appointments, 212,000 lines of payment info, and more.
Tool Sale	An actor on a popular criminal forum was selling what he claimed was a GoCloud Preauth RCE 0day with more than 800,000 vulnerable devices. He did not name a price or further describe the vulnerability. The sales thread was closed by a moderator pending the payment of a USD 10,000 vendor bond.

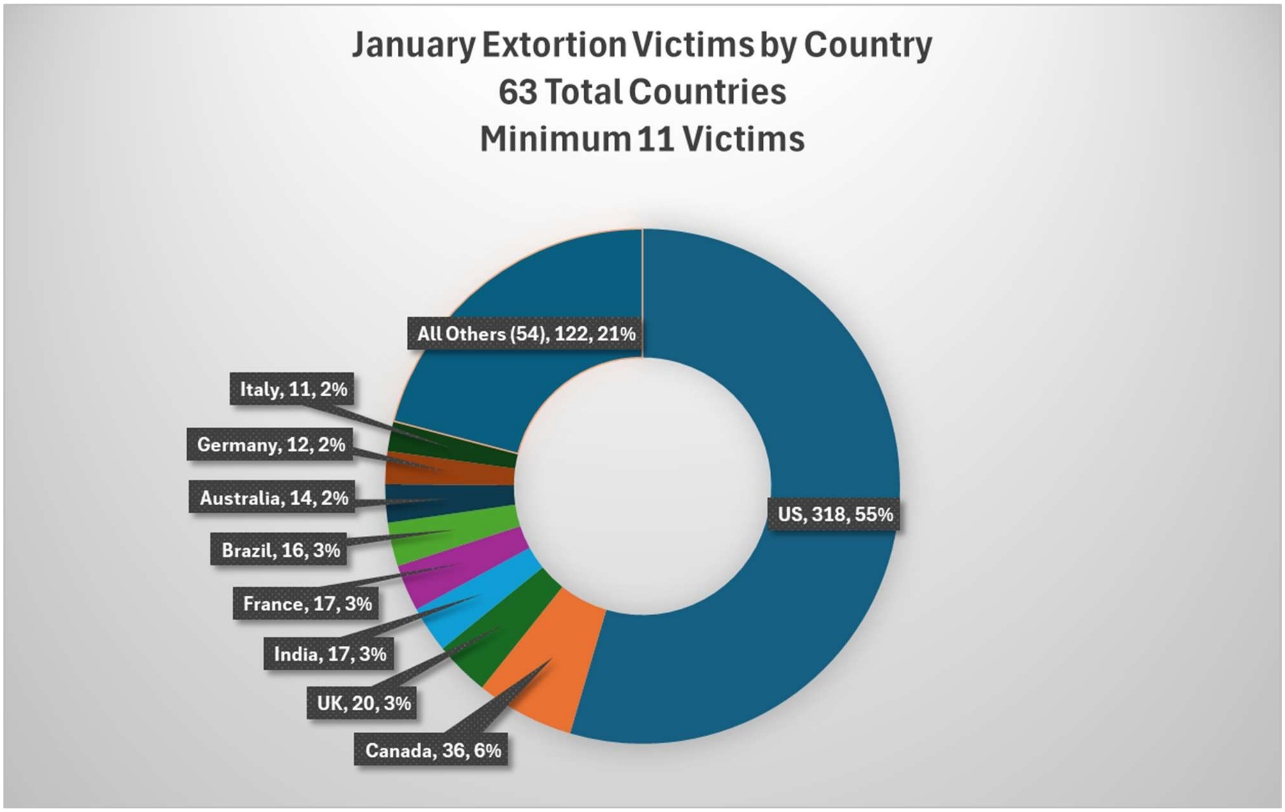
Actor Developments	A new group posted a combo list supposedly containing 15,000 lines of usernames/passwords for FortiGate VPNs for free.
Access Sale	In his first post on Exploit crime forum, an actor announced the inauguration of their access sales service. The first victim was RDweb access to a Connecticut based media and internet company with USD 16.3 million in revenue. He posted poorly redacted screenshots of the ZoomInfo entry and the Windows settings page of the victim.
Access Sale	An access seller was observed selling AnyDesk local admin access to the Harvard University Neurobiology department network for USD 5,000.
Data Sale	An actor on a popular criminal forum sold what he claimed was a database consisting of 10 billion lines of emailpassword to another actor for USD 900. If this is legitimate, it represents one of the largest databases of email|passwords in circulation.

By The Numbers

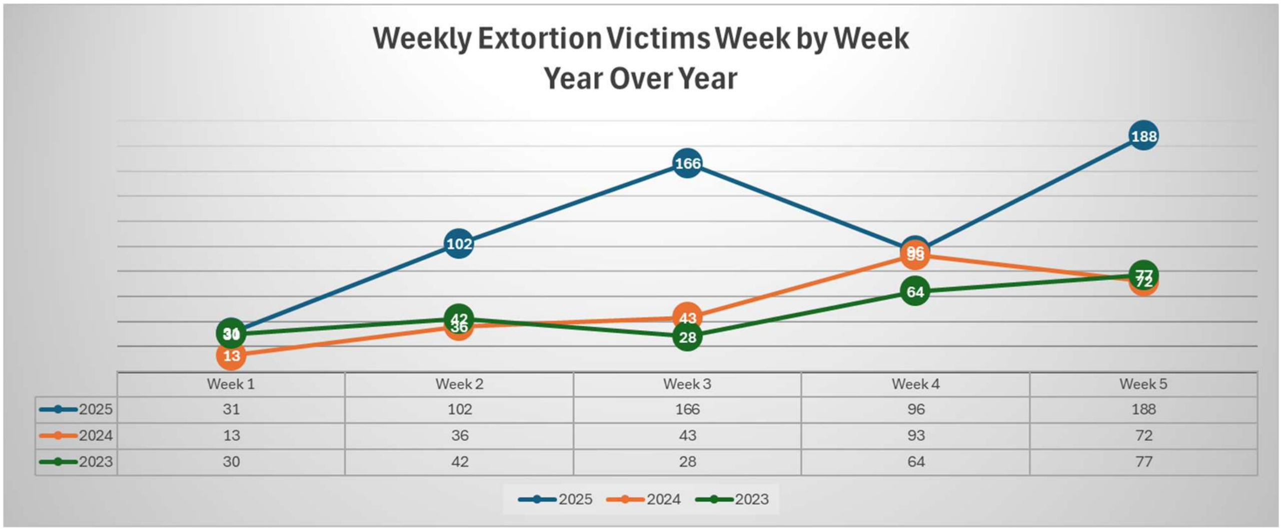
Summarizing incidents in graphical format





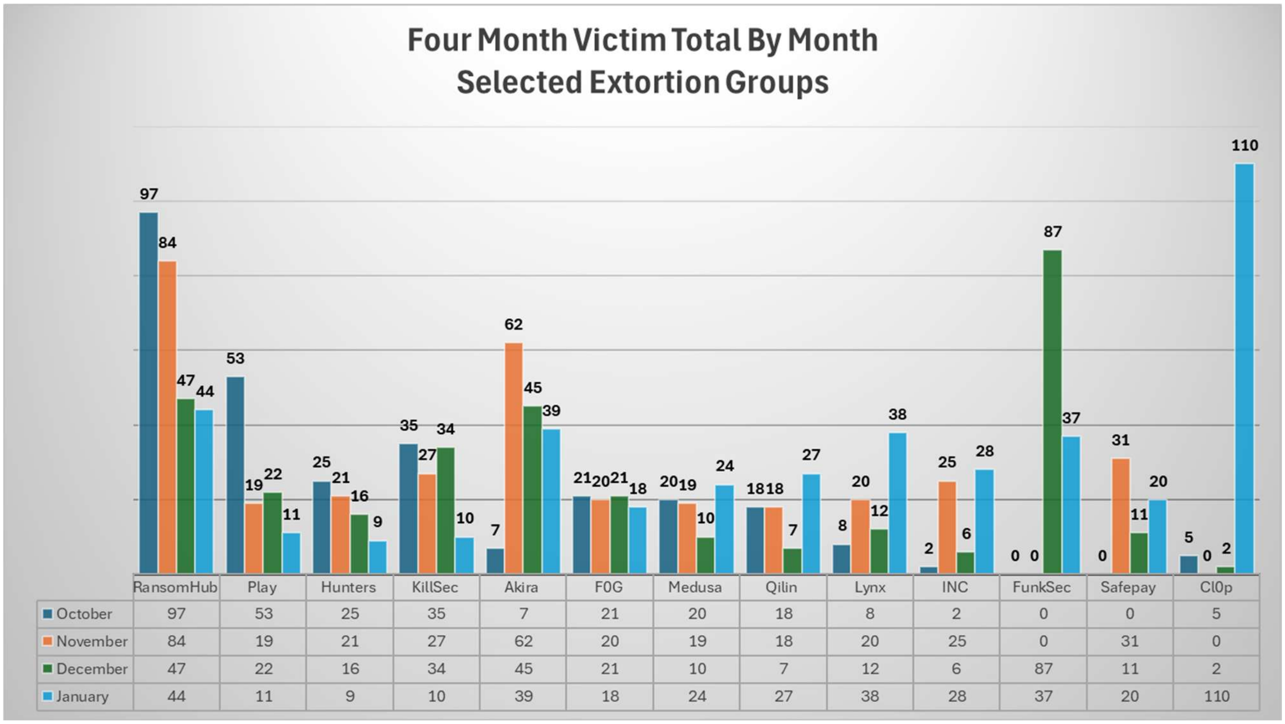


January Extortion Victims by Country
63 Total Countries
Minimum 11 Victims



Weekly Extortion Victims Week by Week
Year Over Year

	Week 1	Week 2	Week 3	Week 4	Week 5
2025	31	102	166	96	188
2024	13	36	43	93	72
2023	30	42	28	64	77



Four Month Victim Total By Month
Selected Extortion Groups

	RansomHub	Play	Hunters	KillSec	Akira	F0G	Medusa	Qilin	Lynx	INC	FunkSec	Safepay	Cl0p
October	97	53	25	35	7	21	20	18	8	2	0	0	5
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

New Detection Content

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

- **Renamed BOINC.exe**
  - BOINC is an open-source software allowing users to donate their computing power to assist scientific research projects. Threat actors have been seen using a renamed BOINC to connect to a C2.
  - **Platforms**: SentinelOne, Carbon Black
  - **Reference**: https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software, https://www.esentire.com/blog/mintsloader-stealc-and-boinc-delivery
- **ESCU - WBAdmin Delete System Backups**
  - This search looks for flags passed to wbadmin.exe (Windows Backup Administrator tool) that delete backup files. This is typically used by ransomware to prevent recovery.
  - **Platforms**: Splunk
- **ESCU - Attempt to Delete Services**
  - This analytic identifies Windows Service Control,"sc.exe," attempting to delete a service. This is typically identified in parallel with other instances of service enumeration of attempts to stop a service and then delete it. Adversaries utilize this technique to terminate security services or other related services to continue their objective and evade detections.
  - **Platforms**: Splunk
- **ESCU - Resize Shadowstorage Volume**
  - This analytic identifies the resizing of shadowstorage using vssadmin.exe to avoid the shadow volumes being made again. This technique is typically used by adversaries during a ransomware event and is a precursor to deleting the shadowstorage.
  - **Platforms**: Splunk
- **Possible Teams Phishing Activity**
  - This rule detects potential Teams phishing activity related to observed attacks where threat actors are impersonating Help Desk support to gain access to a victim's machines remotely.
  - **Platforms**: Microsoft Defender, CrowdStrike

Reference: https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

[i] https://threatbook.io/blog/id/1100

[ii] https://www.fortinet.com/blog/threat-research/burning-zero-days-suspected-nation-state-adversary-targets-ivanti-csa

[iii] https://blog.xlab.qianxin.com/large-scale-botnet-airashi/

[iv] https://www.ispreview.co.uk/index.php/2025/01/uk-internet-domain-registry-nominet-suffers-cyber-attack.html

[v] https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Unveiling-PLAYFULGHOST-with-Google-Security/ba-p/850676

[vi] https://www.cyfirma.com/research/noneuclid-rat/

[vii] https://www.cyjax.com/resources/blog/the-great-morpheus-new-extortion-group-dls-emerges/

[viii] https://www.speartip.com/fasthttp-used-in-new-bruteforce-campaign/

[ix] https://blog.qualys.com/vulnerabilities-threat-research/2025/01/21/mass-campaign-of-murdoc-botnet-mirai-a-new-variant-of-corona-mirai

[x] https://www.broadcom.com/support/security-center/protection-bulletin/mintsloader-campaign-targets-energy-sector-with-stealc-and-boinc-malware

[xi] https://www.zscaler.com/blogs/security-research/technical-analysis-xloader-versions-6-and-7-part-1

[xii] https://cloud.google.com/blog/topics/threat-intelligence/scatterbrain-unmasking-poisonplug-obfuscator

[xiii] https://www.akamai.com/blog/security-research/2025-january-new-aquabot-mirai-variant-exploiting-mitel-phones

[xiv] https://securelist.com/eagerbee-backdoor/115175/

[xv] https://habr.com/ru/companies/f_a_c_c_t/news/874046/

[xvi] https://blog.lumen.com/the-j-magic-show-magic-packets-and-where-to-find-them/

[xvii] https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/

[xviii] https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/

[xix] https://www.cyjax.com/resources/blog/data-leak-site-emerges-for-new-extortion-group-gd-lockersec/

[xx] https://blog.talosintelligence.com/new-tornet-backdoor-campaign/

[xxi] https://www.bitdefender.com/en-us/blog/businessinsights/uac-0063-cyber-espionage-operation-expanding-from-central-asia