
# Monthly Threat Intelligence Rollup

DEEP seas

03/01/25-03/31/25

# Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

| Incident | Activity Summary |
|---|---|
| **Akira Ransomware Group's 'Peeping Tom' Tactic Garners Success** | The S-RM team has recently identified an attack by the Akira ransomware group featuring an unusual initial access method. After compromising a victim's server, Akira attempted to install their ransomware onto the device, but their attempt was blocked by the EDR. To counteract this, Akira performed a network scan and found a vulnerable webcam connected to the victim's network. After compromising this webcam, the attack was able to be carried out as planned and infected the victim's network. Because the webcam was not monitored by security solutions, the increase of SMB traffic was not detected, making it the perfect start to the attack.[i] |
| **The Oracle Has Gone Blind** | CloudSEK has highlighted what may become the biggest supply chain hack of 2025, with the threat actor claiming to have compromised over 140k tenants at Oracle Cloud, successfully exfiltrating around 6 million accounts' authentication-related data. This declaration was made by a cyber criminal forum user who posted SSO & LDAP credentials, OAuth2 keys, and customer tenant information for sale. While Oracle has denied the claim, CloudSEK believes they are mistaken and offered proof as a rebuttal to Oracle. This evidence consists of a script used in the attack that references an Oracle domain for OAuth2 access token generation, real businesses' domains being listed as victims, and a 10,000-line sample of the stolen data. Independent researchers have also investigated the validity of the leak, and most have confirmed it is likely a legitimate breach.[ii] |
| **Clogging Russia's Pipelines** | Reports have come in regarding a large-scale cyber attack this month against the Russian oil giant Lukoil, the second-largest oil producer in the country and an important player in the country's energy industry. This attack resulted in a complete shutdown of the company's internal systems and customer-facing fuel stations in affected areas. Lukoil staff were reportedly shown unusual error messages on their computers and customers have been unable to pay for gas. To add to that, Russia's Fast Payment System (SBP) appears to have suffered a similar outage at the same time, with over 1,500 complaints about SBP within an hour. So far, there has been no official estimate provided on when the systems will be restored. Based on past attacks against Lukoil, their recovery time will likely be around three days.[iii] |
| **Head in the Daisy Cloud** | Veriti research circulated news regarding their find of 30,000 stolen credentials in a telegram group named "Daisy Cloud," which may be associated with RedLine Stealer. The group appears to be financially motivated, targeting cryptocurrency platforms, online entertainment services, cloud infrastructure, education, finance, government, and more. In total, 1,992 hosts, 30,970 account credentials, and 25,693 services tied to credentials were posted by the unknown group linking back to 108 unique countries. The top countries besieged by Daisy Cloud are Vietnam and India, with a focus on aiming for Windows devices. Prices range from $100 for a week of access to their logs, $120 for two weeks, $200 for one month, $600 for three months, and $5,000 for three years.[iv] |
| **Check Point Reportedly Breached** | The Israel-based cybersecurity company Check Point was recently seen possibly suffering a security breach into their internal data and network systems. Asking for around $434k in ransom, the actor stated that they had access to Check Point data such as IP documentation, user credentials, internal network maps and architecture diagrams, source code to Check Point software, and employee PII. Check Point stated that the data comes from an "old, known, and very pinpointed event" in the past, proclaiming the data useless. CoreInjection also has only been seen targeting Israeli entities, demonstrating a possible political motivation as well. Due to Check Point's unusual silence on the matter, the security community is unsure whether to believe their claims.[v] |
| **The Wild West of Ransomware** | A previously unknown threat actor going by "Arkana Security" launched its first ransomware attack against WideOpenWest, one of the largest cable and broadband service providers in the United States. With a network that reaches approximately 1.9 |

| | |
|---|---|
| | million homes and businesses, WOW! serves approximately 538,100 subscribers. The breach reveals that Arkana accessed over 403,000 customer accounts. The details released from these customer accounts are usernames, passwords, security questions, and service package details. The threat actor also seized control of critical WOW! backend infrastructures, including their AppianCloud and Symphonica system, which helps Arkana push malware onto more victim devices, along with manipulate backend code, alter business logic, and modify data flows, including customer financial transactions, personal details, and billing records. Additionally, Arkana can execute unauthorized transactions, access customer accounts, and modify billing information using AppianCloud and Symphonica. Arkana also claims in their post that their capabilities also extend to exfiltrating sensitive data, such as SSNs, credit card information, and more.[vi] |

# Emergent Malware and TTPs

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

| Malware/Campaign | Activity Summary | TTP Analysis |
|---|---|---|
| **Remcos RAT Updated Yet Again** | The SonicWall threat research team has noted new additions to the Remcos RAT, specifically the malware is using both AMSI scanning and ETW logging to evade detection. | The Anti-Malware Scan Interface (AMSI) is a Windows component used to integrate anti-malware software on a device and perform actions such as scanning memory, scripts, content source URLs, and more. Using a custom PowerShell script before any AMSI actions are made, attackers can bypass AMSI. Event Tracing for Windows (ETW), however, is a major logging element of Windows, keeping track of all changes on a device. To bypass this, the attackers target the ntdll.dll function, EtwEventWrite, which logs ETW events, causing the event logger to skip all events without recording data, preventing any malware detections.[vii] |
| **Eleven11bot Continues Trend of Mirai Malware Updates** | GreyNoise has recently identified a new variant of the Mirai botnet, which GreyNoise has designated as "Eleven11bot." | Information gathered by GreyNoise and other security companies points to Eleven11bot being developed by Iran, following sanctions against the country by the United States. So far, Eleven11bot has been used in DDoS attacks against various telecom providers and gaming platforms. To gain initial access, the botnet and actors behind it perform brute-force attacks and open port scanning, and they exploit vulnerabilities in HiSilicon-based devices, specifically those running TVT-NVMS9000 software. With about 1,400 IPs related to the botnet, GreyNoise has determined that 96% of these IPs are non-spoofable and originate from real devices.[viii] |
| **ESP32 Microcontrollers Reportedly Shipped with Backdoor** | Tarlogic Security recently made an alarming discovery in finding a hidden backdoor in ESP32 chips, a microcontroller used for WiFi and Bluetooth connections. | These chips were found to have hidden commands built-in that were not documented by the manufacturer. These commands can perform actions such as device scanning, fuzzing network packets, exploiting low-level protocols, and more. This is concerning because ESP32 chips can be purchased for around $2. In fact, the Chinese semiconductor company Espressif has previously stated that they had one billion worldwide sales of this chip to date.[ix] |
| **Ballista Botnet Targeting IoT Devices Worldwide** | Cato CTRL has published their findings regarding a new botnet targeting IoT devices, designating the botnet as "Ballista." | This name references the Roman siege weapon for two reasons: the attacker's IP originates from Italy and the initial access method is the RCE vulnerability CVE-2023-1389 that targets TP-Link Archer routers. After the router is exploited, a bash script malware dropper downloads the malware. Once run, this secondary payload sets up an encrypted C2 channel to control the device remotely. After achieving this, the attackers have been seen running shell commands to perform actions such as DoS attacks and reading sensitive files on victim devices. So far, Ballista has targeted manufacturing, medical, services, and technology sectors in the United States, Australia, China, and Mexico.[x] |
| **DragonForce Group Alters Tactics** | Independent security researcher Idan Malihi made headlines with his research into the ongoing developments of the DragonForce group and its new ransomware. | The group has changed its modus operandi from hacktivism to cyber criminal operations. One way the group does this is through their ransomware, also named DragonForce. The ransomware was created using a 2022 version of the LockBit builder. The malware is a 32-bit EXE file compiled in C++ that performs expected ransomware activities such as encryption and changing the wallpaper, but also contains defense evasion |

| | | |
|---|---|---|
| | | features, such as terminating EDRs, deleting event logs, and self-deletion. Despite these differences, however, DragonForce ransomware and LockBit ransomware function almost identically. DragonForce also seeks out applications and system or database processes to terminate and encrypt them.[xi] |
| **XCSSET Malware Variant Adds New Features** | Microsoft Threat Intelligence announced their work into dissecting the newest variant of XCSSET. | XCSSET is known as a modular backdoor for macOS that targets Xcode application developers and Xcode projects. This variant of the backdoor features improved error handling and a large increase in the use of scripting languages, commands, and legitimate binaries. The malware demonstrates advancements in its obfuscation, such as obscuring module names, randomized payload generation, and Base64 support. XCSSET also contains new persistence techniques, leveraging methods, tools, Git commits, and more.[xii] |
| **StilachiRAT Proves to Be a Full-Featured Entrant in Malware Toolkits** | Microsoft Incident Response researchers have drawn attention to themselves with the discovery of a new RAT, “StilachiRAT.” | StilachiRAT collects a plethora of information, including browser credentials, OS details, active RDP sessions, running GUI applications, clipboard content, and more. The malware establishes its persistence through the Windows SCM using a watchdog thread for reinstallation if removed. It also attempts to perform lateral movement through RDP sessions by impersonating users. StilachiRAT also makes a good effort to evade detection from event logs, tools, and sandboxes. Once on a device, a C2 connection is established where Stilachi can perform a multitude of commands such as log clearing, system reboots, and more.[xiii] |
| **Rules File Backdoor Targets AI-Generated Code** | Pillar Security researchers unveiled a new supply chain attack that they call "Rules File Backdoor." | This novel technique ignores ethical AI constraints and allows adversaries to stealthily inject prompts into AI-generated code through the AI code editors’ configuration files, including Cursor and GitHub Copilot. The reason for this is to purposefully have the AI generate vulnerable code that can be exploited by the attackers. This is done using invisible Unicode characters that AI can see but humans cannot see, including zero-width joiners and bidirectional text markers. Doing this allows for working around ethical AI constraints, making the AI write vulnerable code. Due to AI configuration files often being shared online, they have become well adopted in the industry and trusted unquestioningly, to the point that the files are rarely validated for vulnerabilities.[xiv] |
| **Arcane Stealer and ArcanaLoader Targets Low-Hanging Fruit** | Kaspersky has posted a follow-up to their initial findings for Arcane information stealer and a new loader called “ArcanaLoader.” | Named by the creators, the Arcane stealer seeks to capture data about all types of information from different applications, including VPNs, the network, IM apps, email clients, gaming clients, and more. The stealer also collects system information, including the OS version, username, computer name, location, drives, anti-virus, and browser data. Paired with Arcane is ArcanaLoader, a loader with a GUI that allows for downloading and running software cracks and more. This, however, is a trick and contains Arcane as a hidden payload within itself.[xv] |
| **Betruger Backdoor Added to RansomHub Affiliate Toolbox** | The Symantec threat hunter team has found a novel backdoor utilized by a RansomHub affiliate known as “Betruger.” | Betruger is a backdoor used to assist in their ransomware deployment. It contains unique attributes for a backdoor, including screenshotting, keylogging, C2 file uploading, network scanning, privilege escalation, credential dumping, and more. A theory given by Symantec regarding its purpose for development was that the backdoor may be used to minimize the number of tools needed on a victim network, reducing RansomHub’s footprint in the victim’s environment. Details about the functionality of this backdoor are sparse but will likely develop if it is seen in more attacks.[xvi] |

| | | |
|---|---|---|
| **ABYSSWORKER Driver Used in Medusa Ransomware Attack** | Elastic Security Labs went into details about a malicious driver used during a Medusa ransomware attack called "ABYSSWORKER." | This loader is a custom-built driver used to disable EDR protections and evade detection or prevention capabilities. Imitating a CrowdStrike Falcon driver, it features other obfuscation techniques such as containing useless functions to muddy analysis. ABYSSWORKER uses DeviceIoControl handlers to issue commands, which include tasks such as copying and deleting files, terminating processes, loading a set API, and more.[xvii] |
| **ClearFake's FlickFix Framework Modified** | The Sekoia Threat Detection & Research team has seen the ClearFake framework go through recent changes. | This change is mainly seen through ClearFake's use of the social engineering tactic ClickFix, a technique that displays fake error messages in the web browser to deceive users into copying and executing a malicious PowerShell to infect their devices. In this case specifically, ClearFake uses fake reCAPTCHA or Cloudflare Turnstile verifications, along with fake technical issues, to trick users into resolving these CAPTCHA challenges to employ ClickFix attacks against them. The framework was also seen adding interactions with the Binance Smart Chain, which allows for JavaScript scripts and other tools to capture data from the victim's device and the downloading, decrypting and displaying of the ClickFix lure. ClearFake is used to deploy further malware such as Emmenhtal Loader, Lumma Stealer, and Vidar Stealer.[xviii] |
| **TINYSHELL Variants Prove UNC3886 Rapidly Iterating on Their Malware** | Mandiant has published their research into the China-nexus espionage group UNC3886 and their new suite of TINYSHELL variants. | In total, Mandiant was able to detect six TINYSHELL variants developed by UNC3886. The first is "appid," an active backdoor that masquerades as a legitimate binary named appidd, also known as the Application Identification Daemon. The second is "to," another active backdoor named after the binary top (Table of Processes). These two backdoors have similar capabilities, including sending and receiving files, launching shells, establish Socks proxies, and more. The third is "irad," a passive backdoor, pretending to be the irsd binary, which stands for Interface Replication and Synchronization Daemon. This backdoor employs a libpcap-based packet sniffer and receives commands by inspecting packets on the wire for certain key words before activating. The fourth is "jdosd," a passive backdoor with a focus on file transfers impersonating jddosd, which is the Juniper DDOS protection Daemon. The fifth is "oemd," which is another passive backdoor targeting network interfaces disguised to look like oamd, or the Operation, Administration and Maintenance Daemon. Finally, there is "lmpad," a utility and passive backdoor, masking as a binary named lmpd, also known as the Link Management Protocol Daemon. This backdoor can launch external scripts that perform process injection into Junos OS processes to prevent logging.[xix] |
| **QWCrypt Signals Shift from Espionage to Crime in RedCurl Group's Operations** | In a recent discovery, Bitdefender Labs found a connection between the RedCurl group and a new ransomware family called "QWCrypt." | QWCrypt, based on the self-reference "qwc'" found within the ransomware executable, demonstrates a massive shift in RedCurl's operation, transitioning from the group's traditional goals of cyber espionage and data exfiltration. The ransomware, like previous RedCurl activity, is delivered through phishing emails containing IMG files disguised as CV documents. Interestingly, after infection, QWCrypt does not attempt to encrypt all available devices as most ransomware would, but instead only targets hypervisors. By encrypting the hypervisor, QWCrypt is attempting to make entire virtualized environments unbootable. The ransomware also especially avoids detection from listed EDRs, such as Windows Defender, Malwarebytes, VIPRE Business Agent, Bitdefender, and |

| | | |
|---|---|---|
| | | SentinelOne.[xx] |
| **CoffeeLoader Executes on GPUs To Avoid Analysis** | Zscaler ThreatLabz has noticed a new downloader going by the title of “CoffeeLoader.” | The many interesting details about the loader start with its packing process, utilizing a custom packer which Zscaler named “Armoury,” that executes code on a system’s GPU to hinder analysis in virtual environments. After unpacking, a dropper for CoffeeLoader is used. This dropper has three variants, each with unique attributes that can perform tasks such as establishing persistence in victim environments. Next comes the staging component, which injects CoffeeLoader into a legitimate dllhost process. The actual malware itself has many notable features, including evading detection from AV and EDR solutions through call stack spoofing, sleep obfuscation, and leveraging Windows fibers. Commands that can be run from CoffeeLoader include a sleep command, injecting or running shellcode in specified processes, updating the sleep obfuscation method, and writing payloads to the victim’s device, and running them through multiple methods.[xxi] |

# Threat Actor Campaigns

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

| Threat Actors | Activity Summary |
|---|---|
| **Campaign Targeting US, Chinese ISPs Emanates from Eastern Europe** | The Splunk Threat Research Team has shed light on a campaign targeting ISPs in the United States and China. This campaign, seemingly coming from Eastern Europe, appears to be financially motivated, with the goal of installing crypto mining malware on victim devices. To do so, the attackers use a toolkit of malware that has capabilities such as brute forcing passwords, deploying additional payloads, self-termination, persistence, disabling services such as Remote Access, C2 data exfiltration, and more. To gain initial access to a potential victim's environment, the group will deploy brute force attacks against ISP infrastructure to gain access to victim accounts. To find these vulnerable machines, masscan was used, a tool which allows for IPs to be scanned at a mass scale, looking for open ports to perform brute force attacks. So far, Splunk has identified over 4,000 IP addresses targeted.[xxii] |
| **UNK_CraftyCamel Targeting Aviation, Telecoms, Transport Companies** | Proofpoint researchers have pointed out a new campaign targeting their customers in the aviation, satellite communication, and transportation industries in the United Arab Emirates. This new group, which Proofpoint calls "UNK_CraftyCamel", originally compromised an Indian electronics company's email account to send legitimate looking spear-phishing emails. The emails contain a malicious URL that linked to a CraftyCamel-controlled domain, which downloads a ZIP archive containing what appears to be an XLS file and two PDF files but are actually other file types such as HTA and further ZIP archives. These files later allow for CraftyCamel's main objective, to deploy their custom Sosano backdoor. Some commands Sosano can perform include getting, changing, and listing of the working directory, downloading and running additional payloads, deleting directories, and executing shell commands.[xxiii] |
| **Phantom Goblin Campaign Makes Heavy Use of GitHub, Telegram** | Cyble Research and Intelligence Labs has proven the existence of a new campaign that they have named "Phantom Goblin." Infection begins when a RAR archive is sent to a victim through phishing. Opening the RAR archive, a LNK file is present disguised as a PDF, which issues PowerShell commands to download a PowerShell script from an attacker-controlled GitHub repository. This script downloads the later payloads and establishes persistence in the Windows Registry. In total, three unique pieces of malware are downloaded, one that uses a Visual Studio Code tunnel to exfiltrate data to the threat actor's Telegram bot, one that steals web browser cookies and avoids Google Chrome's App Bound Encryption, and one that steals data from web browsers. The goal of the campaign is primarily to target web browsers and developer tools to steal data and gain unauthorized access to victim networks.[xxiv] |
| **Japanese Companies Targeted Via PHP Vulnerability** | Cisco Talos has discovered a novel campaign targeting organizations across Japan, directing their focus towards industries such as technology, telecommunications, entertainment, education, and e-commerce. The attack chain of the campaign begins by exploiting CVE-2024-4577, a bug in the PHP-CGI implementation of PHP on Windows that can allow for remote code execution. After the vulnerability has been successfully exploited, a PowerShell script runs a Cobalt Strike reverse HTTP shellcode, backdooring the victim's device. Following this, they collect data on the affected system and then run malware such as JuicyPotato, RottenPotato, and SweetPotato against the machine with said data to gain SYSTEM user access. Persistence is then established by manipulating registry keys, scheduling tasks, and using Cobalt Strike plugins such as TaoWu. To maintain access, the unknown threat actors erase Windows event logs and then finally Mimikatz is used to dump and exfiltrate collected passwords and NTLM hashes to the attacker's C2.[xxv] |
| **OBSCURE#BAT Campaign Deploys Open-Source Rootkit** | The Securonix Threat Research team has been paying close attention to a novel campaign that they have designated as "OBSCURE#BAT." The campaign can begin in a couple ways: a fake captcha that convinces you to run secretly copied commands or disguising their malware as legitimate tools. The attackers then establish persistence by |

| | |
|---|---|
| | manipulating the Windows Registry and Task Scheduler and defense evasion through AMSI patching. The campaign aims to deploy r77, an open-source rootkit. Only some of the many capabilities of this rootkit include process hiding, file masking, kernel interaction, and more.[xxvi] |
| **Mora_001 Group Emerges With 'SuperBlack' Ransomware** | Forescout Research – Vedere Labs has proven the existence of a new ransomware family the company named "SuperBlack." This ransomware has been attributed to a new group Forescout named "Mora_001," because artifacts in the malware are written in Russian. Mora begins its attacks by abusing vulnerabilities in FortiOS devices to escalate privileges. The group then establishes persistence by creating a multitude of accounts on the affected device and manipulates the firewall configuration file. After this, Mora used firewall configurations, dashboard insights, and network connections for lateral movement and WMIC for discovery and execution, along with SSH to access any other potential devices. If all goes well, the SuperBlack ransomware is then installed, which is a variant of LockBit 3.0, also known as LockBit Black.[xxvii] |
| **DollyWay World Domination Campaign Operating Since 2016, Targeting WordPress** | GoDaddy security researchers have connected the dots for a malware campaign they named "DollyWay World Domination," after a snippet in the code. Running since 2016, this campaign has compromised over 20,000 WordPress websites globally. GoDaddy has attributed past campaigns to this one as well, stating that the Master134, the Fake Browser Updates, and CountsTDS campaigns were all run by DollyWay. The campaign targets WordPress websites using techniques such as cryptographically signed data transfers, heterogeneous injection methods, automatic reinfection mechanisms, removal of competing malware, and even through WordPress updates and website repairs. The attacker's goal with compromising these websites is to redirect potential victims to VexTrio or LosPollos scam links through established C2 channels and Traffic Direction System nodes.[xxviii] |
| **UAT-5918 Targets Taiwanese Organizations** | Cisco Talos recently reported on a newly disclosed threat actor they have been tracking since 2023 designated as "UAT-5918." Cisco has labelled the group as an APT group, targeting organizations stationed in Taiwan, hoping to establish persistence within unauthorized environments. For initial access, UAT-5918 usually begins by exploiting N-day vulnerabilities found in various web and application servers that have open Internet-facing ports. Once found, the threat actor uses a collection of open-source tools for further access to the victim's environment. Some of these tools include FScan and In-Swor for reconnaissance, FRP and Neo-reGeorge to create reverse proxy tunnels, Mimikatz for credential harvesting, and much more. Cisco believes the goal of UAT-5918 is information theft.[xxix] |
| **Weaver Ant Group Targeting Telecom Companies in Asia** | Sygnia has laid out the details of a novel China-nexus threat actor titled "Weaver Ant." This group appears to have goals of maintaining persistence on telecommunication providers in Asia and enabling cyber espionage through data theft. Weaver Ant deploys web shells such as an encrypted China Chopper variant and a new webshell Sygnia has designated as "INMemory." They also have been seen using a second stage webshell that functions as a recursive HTTP tunnel tool. This tool allows an attacker to send cURL commands that allow for HTTP tunneling to perform lateral movement.[xxx] |

# Dark Web Markets

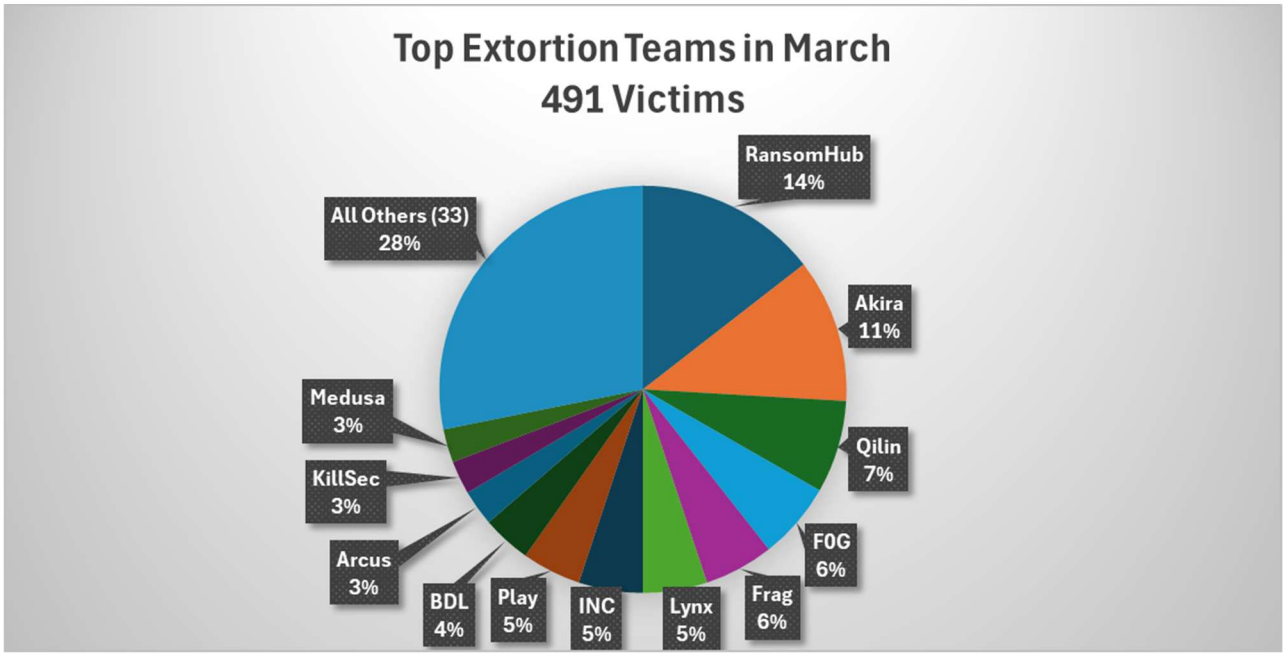
**High-profile ransomware data dumps and dark web access sales identified in last thirty days.**

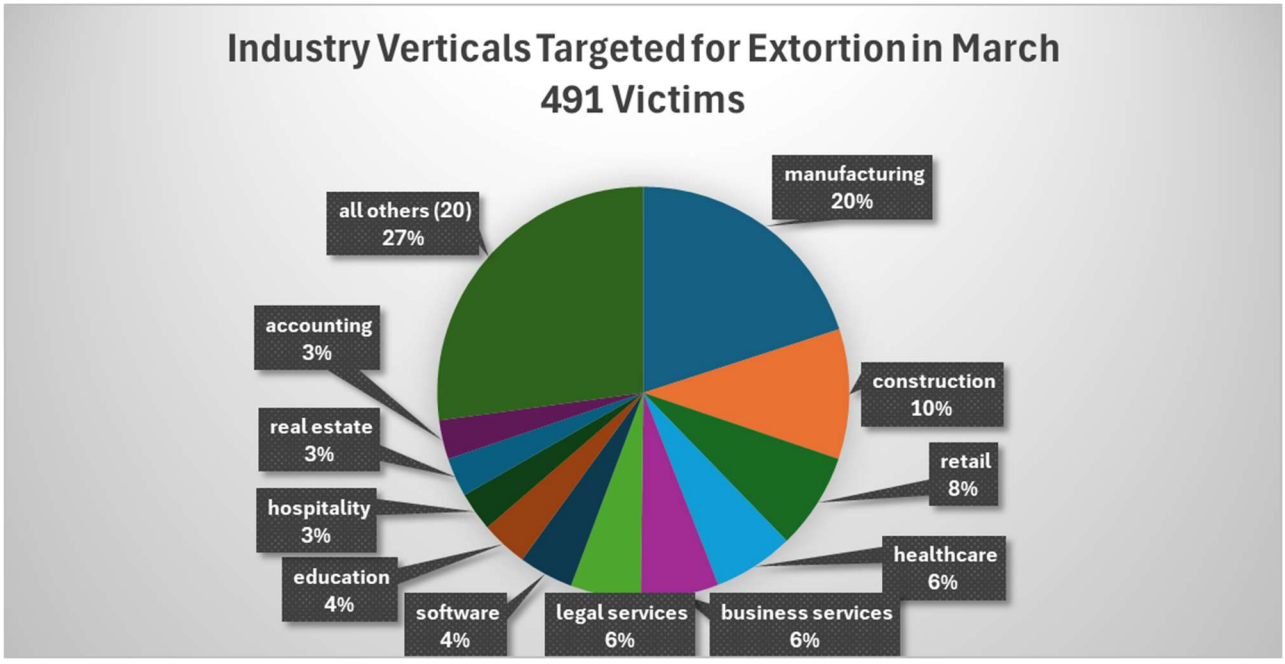
| Activity | Note |
|---|---|
| **Access Sale** | An actor on a popular Russian-language crime forum was selling "bot" access to a US/Japan based manufacturing enterprise with USD 80.6 billion in revenue and 125,111 employees for USD 5,000. |
| **Access Sale** | An access seller on a popular Russian-language crime forum was selling RDWeb local user access to a UK based restaurant group with USD 2.2 billion in revenue for USD 12,000. He closed the sales thread less than a day later. It is unclear if he sold the access or lost access. |
| **Actor Developments** | According to the popular and well-sourced VChK-OGPU Telegram channel – a Russian language social media site covering Russian police and intelligence agencies – the Russian Ministry of Internal Affairs is reportedly discussing cracking down on the RansomHub ransomware team. The report cited a possible RansomHub attack against Russian or allied critical infrastructure by the group, forcing the Russian government to consider taking action. |
| **Access Sale** | A new access seller on a popular Russian-language crime forum was selling firewall access with root privileges to an unnamed cybersecurity company in the US with USD 8.6 billion in revenue for USD 1,300. |
| **Access Sale** | An access seller on a popular Russian-language crime forum was selling VPN domain admin access to a Ghana based data center with USD 108 million in revenue. |
| **Access Sale** | An access seller on a popular Russian-language crime forum was selling admin access to a US based telecommunications company with USD 38.1 million in revenue for USD 1,000. |
| **Access Sale** | An access seller was observed selling VPN access to a South Korea based automobile parts manufacturer with USD 3.7 billion in revenue for a negotiated price. |
| **Access Sale** | An actor on multiple crime forums was offering access to at least 65 companies through an alleged compromise of their Fortinet VPNs. |
| **Tool Sale** | An actor on a long-established crime forum was selling what he claimed was a critical RCE vulnerability in Microsoft Windows affecting the Management Console component. The package included web bypass and a UAC bypass exploit. Price was USD 10,000. Microsoft addressed CVE-2025-26633 in the last patch Tuesday update. Microsoft noted that they've seen exploitation in the wild, however there does not appear to be a publicly available proof of concept. |
| **Access Sale** | An access seller on a popular Russian-language crime forum was selling RDWeb access to a UK based sporting goods retailer with USD 37 million in revenue for USD 4000. |
| **Access Sale** | A new actor on a popular Russian-language crime forum was selling what he described as “high privilege access to the Defense Logistics Agency network” for USD 12,000. He provided six screenshots purporting to demonstrate access, including access to classified information. The screenshots did not appear authentic, and the claim of access is dubious. |
| **Access Sale** | An access seller and probable Hellcat team associated actor was selling VPN credentials to a US based global food processor with USD 7 billion in revenue for USD 400. |
| **Access Sale** | An access seller on a popular Russian-language crime forum was selling domain access to the American branch of "an old [Japan based] company everyone here knows well" for USD 10,000. He additionally claimed he can supply domain admin access to at least 8 companies per week as a supplier. |

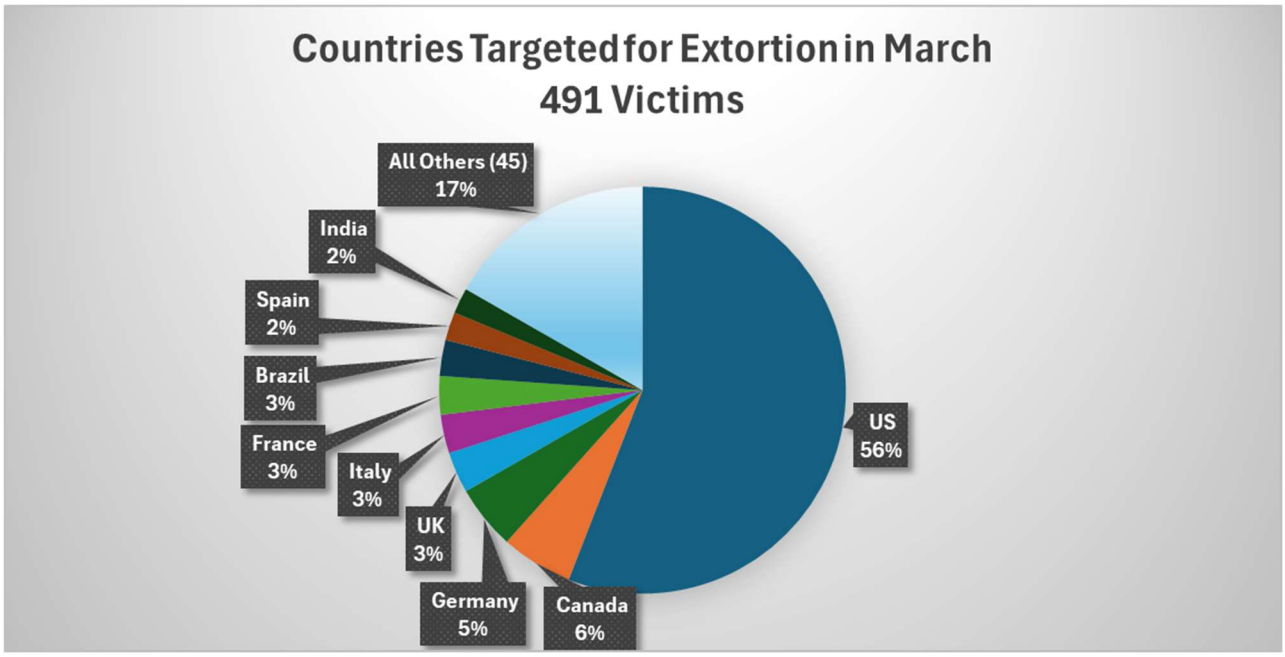
| | |
|---|---|
| **Access Sale** | An actor on a popular Russian-language crime forum was selling Citrix access to a hospitality property in King of Prussia, Pennsylvania. He posted a sample reservation as proof of access. He also posted screenshots, one of which was labeled "modules" showing icons for dozens of other hotel properties throughout the northeast from Pennsylvania to Massachusetts. |
| **Actor Developments** | An actor on a popular Russian-language crime forum was looking to buy email access to @SGS.com, a Switzerland based inspection, verification, testing, and certification company for USD 100 or more. He didn't explicitly say why he wants this access, although it's plausible he is attempting to phish a customer of SGS's, commit BEC against SGS, or even commit industrial espionage. |
| **Access Sale** | An actor on a popular Russian-language crime forum was selling Fortinet user access to a US based financial company with USD 128.9 million in revenue for USD 2,500. He was banned for unknown reasons after posting. |
| **Access Sale** | An actor was observed selling domain user VPN and RDP access to a Virginia based internet service provider with USD 1.4 billion in revenue for USD 1,200. |
| **Access Sale** | An actor was observed selling full access to 250 GB of user data for a major unnamed Australia based retailer with USD 2.6 billion in revenue for a starting price of USD 1,500. He posted multiple screenshots purporting to demonstrate access. |
| **Access Sale** | An actor on a popular Russian-language crime forum was selling domain user Fortinet access to a US based jewelry and watch retailer with USD 41.4 million in revenue for a buy now price of USD 1,400. |
| **Access Sale** | An actor on a popular Russian-language crime forum was selling local admin access to what he described as "the representative office of Puerto Rico in the USA housing administration" with revenue of USD 64 million for USD 2,500. Another actor put in the buy now bid of USD 2,500. |

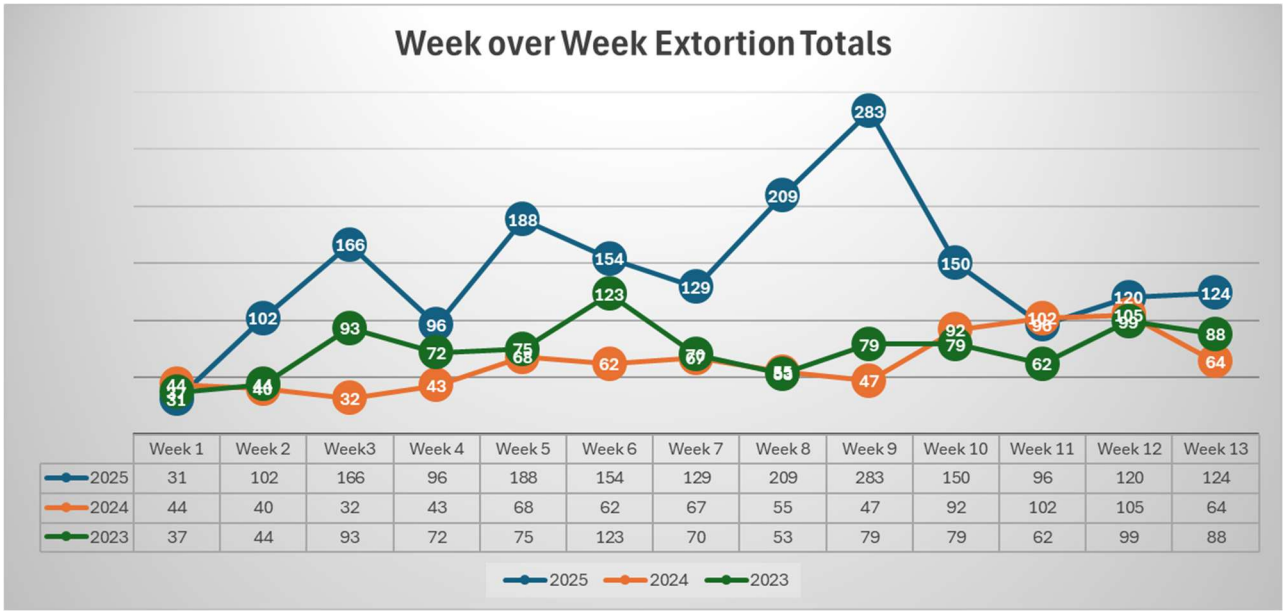
# By The Numbers

Summarizing incidents in graphical format

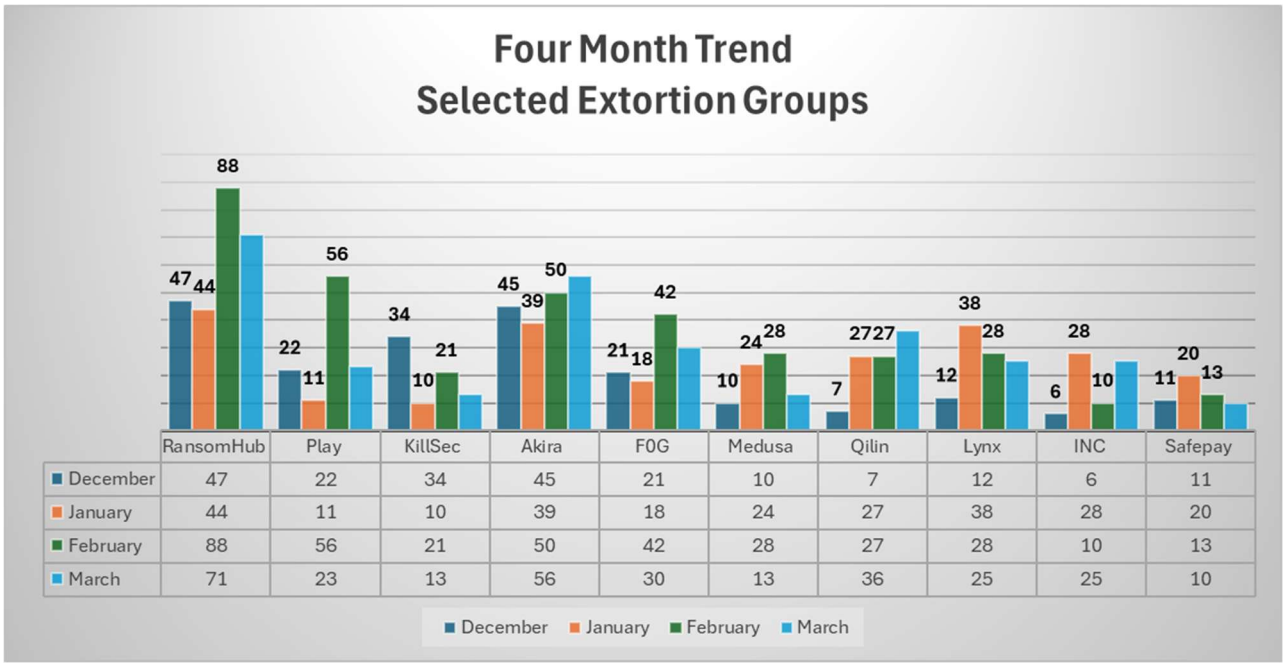





| | Week 1 | Week 2 | Week3 | Week 4 | Week 5 | Week 6 | Week 7 | Week 8 | Week 9 | Week 10 | Week 11 | Week 12 | Week 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2025 | 31 | 102 | 166 | 96 | 188 | 154 | 129 | 209 | 283 | 150 | 96 | 120 | 124 |
| 2024 | 44 | 40 | 32 | 43 | 68 | 62 | 67 | 55 | 47 | 92 | 102 | 105 | 64 |
| 2023 | 37 | 44 | 93 | 72 | 75 | 123 | 70 | 53 | 79 | 79 | 62 | 99 | 88 |




| | RansomHub | Play | KillSec | Akira | F0G | Medusa | Qilin | Lynx | INC | Safepay |
|---|---|---|---|---|---|---|---|---|---|---|
| December | 47 | 22 | 34 | 45 | 21 | 10 | 7 | 12 | 6 | 11 |
| January | 44 | 11 | 10 | 39 | 18 | 24 | 27 | 38 | 28 | 20 |
| February | 88 | 56 | 21 | 50 | 42 | 28 | 27 | 28 | 10 | 13 |
| March | 71 | 23 | 13 | 56 | 30 | 13 | 36 | 25 | 25 | 10 |

# New Detection Content

Noteworthy new detection logic added in the last 30 days, excluding rule tuning.

- **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

- **UNC4393 Tools and Techniques**
  - UNC4393 is a financially motivated threat actor primarily using BASTA ransomware. They have been active since early 2022 and have targeted over 40 organizations across various industries. UNC4393 has shown a willingness to cooperate with other threat clusters for initial access and has evolved from using existing tools to developing custom malware. They focus on efficient data exfiltration and multi-faceted extortion, often utilizing tools like COGSCAN and RCLONE for reconnaissance and data theft.
  - **Platforms:** CarbonBlack, SentinelOne

- **EDRKillShifter - EDR Disabling Tool**
  - Looking for the EDRKillShifter tool used by ransomware actors to disable EDR.
  - **Platforms:** CarbonBlack, SentinelOne, Defender, CrowdStrike

- **Suspected Akira Ransomware File Names**
  - Looking for encrypted files and ransom note file names seen used by the Akira Ransomware group. File modifications with names such as .akira or akira_readme.txt should be examined if this alerts.
  - **Platforms:** CarbonBlack, Defender

- **Suspicious RMM Remote Connection**
  - Looking for remote access connections from Remote Monitoring and Management (RMM) software to suspicious top level domains. Detection looking for a list of (RMM) tools that could be abused by threat actors if not approved software in the environment. List is looking for RMM tools such as: Ammyy Admin, AnyDesk, Atera, GoTo, ITarian RMM, NinjaRMM, ScreenConnect, Splashtop, TeamViewer, VNC, Windows Remote Assistance.
  - **Platforms:** CarbonBlack, Defender, CrowdStrike

[i] https://s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam
[ii] https://cloudsek.com/blog/part-2-validating-the-breach-oracle-cloud-denied-cloudseks-follow-up-analysis
[iii] https://united24media.com/latest-news/russian-lukoil-hit-by-major-cyberattack-disrupting-operations-nationwide-7075
[iv] https://veriti.ai/blog/inside-daisy-cloud-30k-stolen-credentials-exposed
[v] https://hackread.com/hacker-breach-check-point-cybersecurity-firm-access
[vi] https://socradar.io/arkana-ransomware-attack-on-wideopenwest
[vii] https://sonicwall.com/blog/remcos-rat-targets-europe-new-amsi-and-etw-evasion-tactics-uncovered
[viii] https://greynoise.io/blog/new-ddos-botnet-discovered
[ix] https://tarlogic.com/news/hidden-feature-esp32-chip-infect-ot-devices
[x] https://catonetworks.com/blog/cato-ctrl-ballista-new-iot-botnet-targeting-thousands-of-tp-link-archer-routers
[xi] https://idanmalihi.com/dragonforce-ransomware-unveiling-its-tactics-and-impact
[xii] https://microsoft.com/en-us/security/blog/2025/03/11/new-xcsset-malware-adds-new-obfuscation-persistence-techniques-to-infect-xcode-projects
[xiii] https://microsoft.com/en-us/security/blog/2025/03/17/stilachirat-analysis-from-system-reconnaissance-to-cryptocurrency-theft
[xiv] https://pillar.security/blog/new-vulnerability-in-github-copilot-and-cursor-how-hackers-can-weaponize-code-agents
[xv] https://securelist.com/arcane-stealer/115919
[xvi] https://security.com/threat-intelligence/ransomhub-betruger-backdoor
[xvii] https://elastic.co/security-labs/abyssworker
[xviii] https://blog.sekoia.io/clearfakes-new-widespread-variant-increased-web3-exploitation-for-malware-delivery
[xix] https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers
[xx] https://bitdefender.com/en-us/blog/businessinsights/redcurl-qwcrypt-ransomware-technical-deep-dive
[xxi] https://zscaler.com/blogs/security-research/coffeeloader-brew-stealthy-techniques
[xxii] https://splunk.com/en_us/blog/security/infostealer-campaign-against-isps.html
[xxiii] https://proofpoint.com/us/blog/threat-insight/call-it-what-you-want-threat-actor-delivers-highly-targeted-multistage-polyglot
[xxiv] https://cyble.com/blog/phantom-goblin-covert-credential-theft
[xxv] https://blog.talosintelligence.com/new-persistent-attacks-japan
[xxvi] https://securonix.com/blog/analyzing-obscurebat-threat-actors-lure-victims-into-executing-malicious-batch-scripts-to-deploy-stealthy-rootkits
[xxvii] https://forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo
[xxviii] https://godaddy.com/resources/news/dollyway-world-domination
[xxix] https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan
[xxx] https://sygnia.co/threat-reports-and-advisories/weaver-ant-tracking-a-china-nexus-cyber-espionage-operation