
# Monthly Threat Intelligence Rollup

DEEP seas

02/01/24-02/29/24

# Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

| Incident | Activity Summary |
|---|---|
| **Canadian Pipeline Company Affected by ALPHV Ransomware** | Details of a recent compromise of a Canadian pipeline company servicing the petrochemical industry have come to light nearly three months after the incident occurred. Sometime in November 2023, the ALPHV (aka Black Cat) ransomware group compromised an unknown number of systems belonging to Trans-Northern Pipelines (TNPI).The impact was reportedly limited to a small number of internal computer systems according to TNPI. Reportedly, ALPHV stole some 183 gigabytes of internal company documents and has now published them on their extortion site. The long delay suggests that the group was negotiating with Trans-Northern Pipelines for some time; though delays related to the holiday season (both in the west and in Russia) may have led to an excessive delay. Still, it is likely that TNPI spent some time in negotiations before the ALPHV group posted the stolen data publicly. While it is tempting to draw parallels to the Colonial Pipeline incident, there was reportedly no impact to production, transport, or storage of petrochemical products. While it is highly likely that Canadian authorities are actively working with the U.S. FBI to share data regarding this incident in the hopes of prosecuting ALPHV operators, the group has survived takedown efforts before. Still, the announcement of a $10,000,000 bounty on the group's leadership by the U.S. government may prove attractive enough to entice a turncoat. The $5,000,000 bounty on affiliates is also likely to impact the group's recruitment as well.[i] |
| **i-SOON Contractor Leak Exposes Scale of Chinese Espionage Operations** | In mid-February 2023, the information security community became aware of a GitHub repository containing reams of sensitive and proprietary data belonging to i-SOON, a China-based company providing malware development and campaign operation services to the Chinese government. Included in the leaked data were copies of the group's tools, malware, a target list, operations manuals, and other highly sensitive data revealing the company's involvement in a long-running campaign targeting telecommunications companies worldwide and demonstrating that the actors were capable of many things - including operating social media accounts without the owner's knowledge or consent, pilfering and scanning the contents of entire email inboxes, automated penetration testing, and many other capabilities. A translated copy of the target list discovered in the i-SOON leaked data reveals the extent and breadth of Chinese nation-state espionage ambitions. While government agencies, academia, and healthcare are represented in the list, most targets are telecommunications companies (though some of these are government-operated). Some of the nations targeted are to be expected - Taiwan, Pakistan, Hong Kong, and Nepal, but also Kazakhstan, Thailand, Malaysia, Turkey, France, Burma/Myanmar, Nigeria, and Egypt, among others. This suggests that i-SOON either operates at the behest of multiple branches of the Chinese MPS or that multiple branches of the MPS corresponding to multiple disparate APT groups are operating in concert. This breach has given security experts a detailed look at the inner workings of one of the many companies supporting Beijing's nation-state threat actor groups. Undoubtedly more exist, as known victims and nations that have experienced hacking by Chinese nation-state groups are not present in this list. It may be some time before these come to light however, as, undoubtedly, other contracted firms are seeking to ensure that their own proprietary data is not sitting out in the public domain.[ii] |
| **Volt Typhoon Found to be Lurking in U.S. Critical Infrastructure for Over Five Years** | A 7 February report by CISA outlines recent discoveries with regards to the Chinese nation-state Volt Typhoon actor, specifically that they group has been present on the networks of multiple critical infrastructure entities in the United States and Canada for at least five years, if not longer. The Chinese actors have heavily targeted the communications, energy, transportation, water/wastewater sectors in the continental United States and outlying territories, and, given the integration with Canadian infrastructure, the threat extends north of the border as well. As is common with Chinese nation-state actors, use of legitimate and pre-existing tools is common, as is their use of |

| | |
|---|---|
| | zero-day vulnerabilities, extensive reconnaissance of targets before, during, and post-compromise, lateral movement and full domain compromise, credential theft, and in this case, targeting of operational technology assets. One pitfall noted by third parties in CISA's analysis is that often tools and scripts utilized by other actors are not cleaned up properly after an incident, thus some of the potential artifacts observed and reported by CISA may be spuriously contaminating their analysis. A recent report on targeting of vulnerable routers and other network devices was not incidental; these devices were and presumably are still being utilized by Volt Typhoon for command and control.[iii] |

# Emergent Malware and TTPs

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

| Malware/Campaign | Activity Summary | TTP Analysis |
|---|---|---|
| **Rhadamanthys Stealer Targeting ONG Sector** | In January 2024, Cyberint published details of a campaign targeting the oil and natural gas sector with the Rhadamanthys stealer; though no samples of the malware were provided. | This campaign recently surfaced again in the news cycle, and DeepSeas analysts were able to identify a recent sample of Rhadamanthys (version 0.5.2) that incorporates minor improvements made by the developers. Newer versions of Rhadamanthys may be easier to detect, as the malware utilizes Telegram for notifications of exfiltrated data, password theft, and other functions. Testing of the Rhadamanthys stealer against DeepSeas detections demonstrates a high detection rate; nearly 275 separate rules alerted on a sample from this time frame. This handily demonstrates that novel malware developments may not necessarily result in higher success rates; for all the tools and options and features in the world mean very little if the malware is handily detected. Many of the DeepSeas detection rules that alerted on the new sample of Rhadamanthys date back several years, strongly suggesting that the authors have been more intent on adding new features and capabilities rather than improving the malware's stealth and longevity.[iv] |
| **Victims in Mexico Fall Prey to New TimbreStealer Malware** | Reported on 27 Feb by Cisco Talos, a new malware family was discovered which Cisco Talos has named TimbreStealer. | TimbreStealer is described as a new information stealer that has been used to target potential victims in Mexico. TimbreStealer is often used in tandem with phishing emails posing as financial invoices for delivery and has been observed doing so since Nov 2023. Through Cisco Talos' investigations and findings, TimbreStealer has shown its advanced methods of evasion detection. Some of the tactics include using direct system calls to evade API monitoring, implementing the "Heaven's Gate" technique of running 64-bit code within a 32-bit process, and deploying custom loaders. Cisco Talos also discovered multiple modules integrated into the TimbreStealer's ".data" segment, along with a sophisticated decryption procedure. The process entails a primary orchestration DLL and a universal decryption key utilized across the various modules, with updates occurring at each phase. Cisco Talos' investigation on the stealer remains ongoing.[v] |
| **Novel Lambda Ransomware Variant: Synapse Ransomware** | On 12th Feb, X user @rivitna2 disclosed a new variant of the known Lambda ransomware, Synapse, or "Exotic", as it is called in file path to the Synapse PDB file "D:\Projects\Exotic Ransomware - Debug\Release\Crypter.pdb". | In the past, Lambda was known to be associated with the VoidCrypt ransomware group. Due to being brand new to the malware scene, not much information regarding Synapse is available; therefore, a confirmed connection to VoidCrypt has not been made as of now. Synapse operates similarly to other ransomware families, by encrypting data which renders the files unusable and then demanding payment for the decryption. However, @rivitna2 did upload a sample of this variant which DeepSeas has investigated. Sandboxing the file revealed quite a few characteristics of the malware, such as attempting to disable or restrict access to Windows Event Logging, its ability to spread through Windows file shares, and much more. Reverse engineering analysis also disclosed connections between Synapse and other ransomware families, Ironcat and |

| | | |
|---|---|---|
| | | Lorenz, due to their similar ransomware notes.[vi] |
| **New DSLog Backdoor Exploits Recent Ivanti Vulnerability** | On 4 Feb, Orange Cyberdefense released a report regarding a novel backdoor that they have named DSLog due to the malware inserting itself into a Perl file called “DSLog.pm,” a file associate with Ivanti. | This backdoor was used against a recently discovered vulnerability, CVE-2024-21893, which is a server-side request forgery vulnerability in the SAML component of various version of Ivanti products, such as Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons for ZTA. Exploiting this vulnerability allows for an attacker to access restricted resources without authentication, or in this case inject the DSLog backdoor. A notable feature of DSLog is the malware’s ability to implement access control to itself through an API key mechanism which uses a unique hash for each device, meaning that a key cannot be used to contact the backdoor if the key has already been used on another device. As of now, the users and creators of this backdoor have not been disclosed.[vii] |
| **Raspberry Robin Malware Quickly Adopting New Exploits** | A recently published analysis of the Raspberry Robin malware by Check Point has revealed that, while the malware itself remains largely the same, the actors behind the info stealing worm have improved their process for identifying and implementing exploits for recent vulnerabilities. | Case in point, CVE-2023-29360 was disclosed in June 2023, and two weeks later the group had a working exploit implemented. It was not until the end of September 2023 that a public proof of concept exploit was released on GitHub. A working exploit for this vulnerability was sold on dark web forums in February 2023, though presumably not to Raspberry Robin developers. Similarly, CVE-2023-36802 was disclosed in mid-September 2023, and by early October the malware developers had implemented an exploit, though only leading public exploit disclosure by several days in this instance. Several interesting features were noted in the malware itself - the ability to block system shutdown until the malware has fully installed itself, the use of PowerAdmin instead of PsExec, heavy obfuscation, and testing network connectivity prior to beacon attempts. As the malware's C2 attempts to reach out to Tor sites, beaconing activity is still easily detected.[viii] |

# Threat Actor Campaigns

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

| Threat Actors | Activity Summary |
|---|---|
| **Pyongyang Targeting Russian Ministry of Foreign Affairs** | The North Korean state-aligned Konni group, part of the larger nexus of threat actors under Pyongyang's Reconnaissance General Bureau (RGB) termed the Lazarus Group by security companies and researchers, has been observed conducting operations against the Russian Foreign Ministry. While one might be forgiven for thinking that putative allies would restrain themselves from targeting one another, this is not the case with North Korea and Russia. The Russian Foreign Ministry has been targeted by Pyongyang since at least 2021, with other Russian entities, including the Rubin Design Bureau and multiple shipyards, targeted by Pyongyang as well. Similar to a 2023 campaign utilizing backdoored Russian-state mandated tax software, this campaign utilized a backdoored installer for a tool internal to the Russian foreign ministry itself. While this is quite the coup for North Korean actors, the malware itself is quite pedestrian. The developers have not added any new, novel, or interesting features to the malware in quite some time, suggesting that the tool has reached a state where only minor changes are necessary to accomplish the attackers' goals. The target of choice largely matches those of a nation-state intent on espionage; the briefs and documents circulating in a foreign ministry's consular office reporting system would make for a valuable source of intelligence. The fact that North Korea is targeting a putative ally is also unsurprising; there are no friends in the world of politics, only those entities that align with stated goals.[ix] |
| **Kazuar Implant Receives New 'Pelmeni' Wrapper Component** | A recent Lab52.io report provides details of a new component developed by the Russian-state aligned Turla Group, which provides additional obfuscation for the group's signature Kazuar backdoor malware. First detected in samples dating to late January and early February 2024, the Kazuar backdoor now features a wrapper component dubbed Pelmeni by Lab52.io researchers. The Pelmeni wrapper is delivered as a DLL and features heavy obfuscation, encryption of the DLL file's contents, randomly generated exported function names, and multiple execution workflow redirections. More importantly, Pelmeni appears to be used (thus far at least) in highly targeted fashion. If the system name does not match the name that the Pelmeni component is expecting the execution will fail. The Kazuar backdoor itself is largely the same as previous versions; though it does use the socket protocol for data exfiltration, as well as the minor change of storing output logs in a different location.[x] |
| **Unique Use of Steganography in UAC-0184 Attacks** | As recently as 26 Feb., the team at Morphisec Threat Labs has released information about multiple attacks done by UAC-0184, a threat group that is believed to be Russia-affiliated. These attacks were performed using an overlooked method of concealment, utilizing steganography to obfuscate the malware loader used by UAC-0184 (IDAT loader) in the attack to deliver Remcos RAT. These attacks were first spotted by Morphisec in Jan. 2024, with the first step being a phishing email from UAC-0184 to the victim claiming to be an Israel Defense Forces (IDF) consultant. While UAC-0184, in this case, targeted the country of Finland rather than Ukraine, the attack was still related to Ukraine, as UAC-0184's main targets were Ukraine entities based in Finland. After opening the malicious email, IDAT loader is installed on the victim's device, which then begins its process for downloading the final payload. The loader then employs the use of a steganographic PNG embedded in the loader to locate and extract the Remcos payload.[xi] |
| **APT Group, Water Hydra, Takes Advantage of Microsoft Defender SmartScreen Zero-Day** | On 13 Feb., the Trend Micro Zero Day Initiative uncovered a new vulnerability, going by CVE-2024-21412, within Microsoft Defender SmartScreen that allows for an unauthenticated adversary to send victims maliciously crafted files that are designed to bypass displayed security checks. This vulnerability was recently exploited by the APT group, Water Hydra, to target financial market traders through spear phishing. This aligns with Water Hydra's activity in the past, as since 2021 they have made a name for themselves for targeting the whole financial industry at large, not just individual stockbrokers. For instance, they have also been seen attacking brick-and-mortar |

| | |
|---|---|
| | businesses such as banks and casinos, along with online corporations such as cryptocurrency and stock trading platforms, all around the world. Ironically, Microsoft Defender SmartScreen is used to protect against phishing and the downloading of potentially malicious files. Thankfully, however, the attacker would have to convince them to act by clicking on the file link, due to them having no way to force a user to view the attacker-controlled content. It is also worth noting that as of now, this CVE has been patched, and it is recommended by Microsoft to update SmartScreen accordingly.[xii] |
| **Multiple APT Groups Exploiting Fortinet Zero-Day Vulnerabilities** | Reviews of multiple alerts provided by Fortinet regarding older vulnerabilities in their products (principally CVE-2022- and CVE-2023- ) were released this week, along with a critical CVSS ranked 9.6 severity vulnerability in FortiOS (CVE-2024-21762). By Fortinet's own admission, the release of the alert for CVE-2024-21762 was timed to coincide with Volt Typhoon alerts from CISA, all but confirming a link between the two. Review of the alerting from Fortinet shows widespread use by nation-state actors; APT31, APT15, UNC757, the Lorenz ransomware group, and Volt Typhoon were all observed exploiting these zero-day vulnerabilities against various targets, including service providers (APT31), consultants (APT15), and manufacturing local governments (Volt Typhoon). While Fortinet did provide a great number of file hashes and samples, nearly all of them are legitimate tools being abused, open-source penetration testing tools, and other common assets widely utilized by nation-state actors and cyber criminals alike. The recent zero-day in FortiOS is severe and under active exploitation by Volt Typhoon, and the only workaround available for those users unable to patch is to disable SSL VPN entirely, a most unacceptable option for FortiOS users.[xiii] |

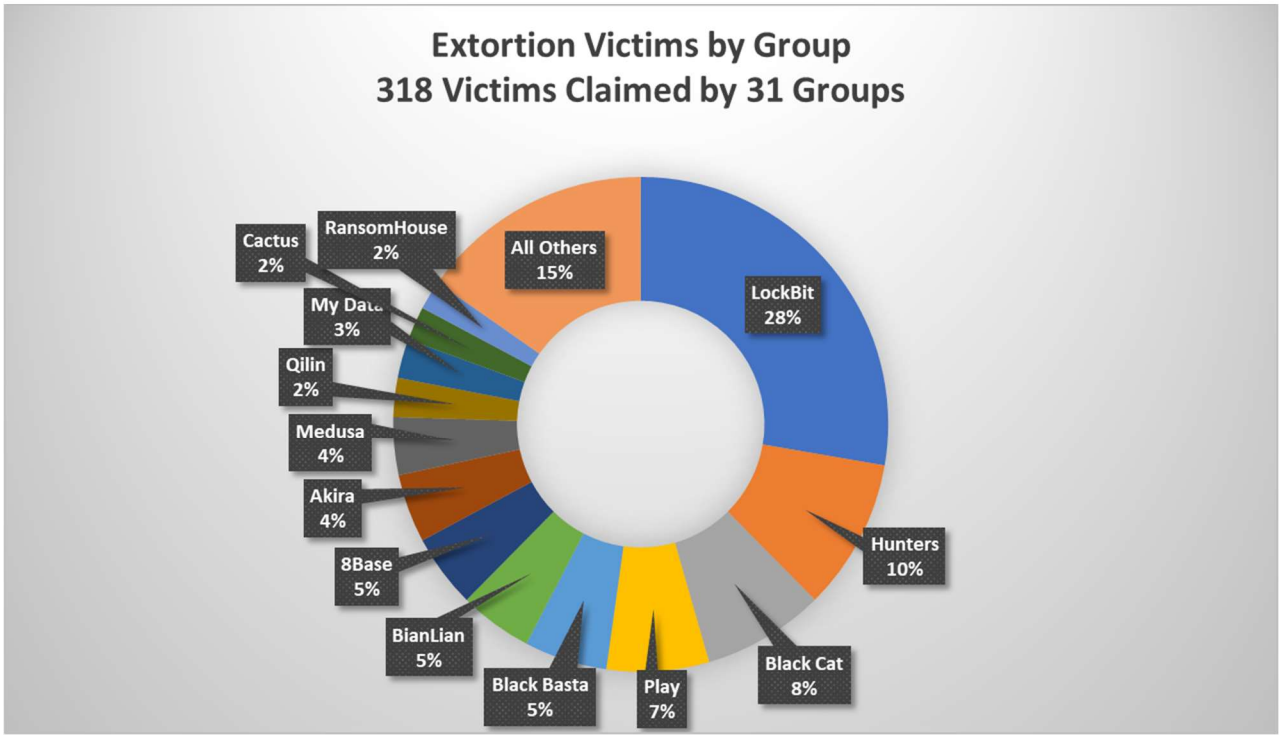
# Dark Web Markets

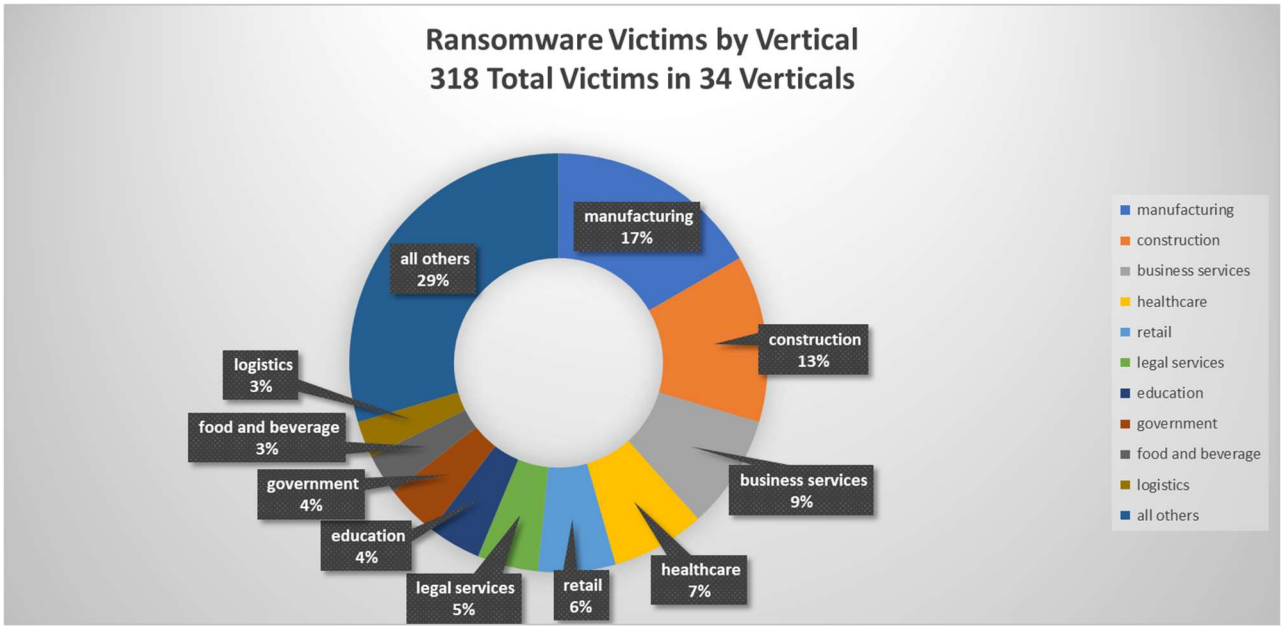
**High-profile ransomware data dumps and dark web access sales identified in last thirty days.**

| Activity | Note |
|---|---|
| **Access Sale** | A Russian speaking actor on a Russian language crime forum was selling Cloud panel access to a Texas based commercial and residential construction company with USD 1.1 billion in revenue for USD 30,000. |
| **Access Sale** | A Russian speaking actor on a crime forum was selling ScreenConnect RDP access with local and domain admin to a U.S. based "manufacturing general" company with USD $2.7 billion in revenue for USD 5,000. |
| **Access Sale** | A Russian speaking actor on a crime forum was selling RDP domain admin access to a Denmark based company in the marine shipping and transportation vertical with USD 4.2 billion in revenue for USD 8,000. |
| **Access Sale** | A Russian speaking actor on a crime forum was selling Plesk hosting control panel access to an information services company with USD 823.9 million in revenue with access to WordPress and two domains and 35 GB of traffic/month for USD 1,000. |
| **Access Sale** | An actor on a Russian language crime forum was selling RDP local user access to a Brazil based logistics company with USD 7.8 billion in revenue for USD 1,500. |
| **Access Sale** | An actor on a Russian language crime forum sold Palo Alto Global Protect user access to a Belgium based food manufacturer with USD 2.2 billion in revenue and more than 9,500 employees for USD 1,500. The same actor was selling Citrix user access to a Dominican Republic based telecommunications company with USD 195 million in revenue and more than 939 employees for USD 800. |
| **Access Sale** | An actor on a crime forum was selling Citrix access to an unnamed France based company with USD 6.7 billion in revenue for a buy now price of USD 2,000. He closed the auction without announcing a winner. |
| **Access Sale** | An actor on a crime forum was selling RDP admin access to a U.S. based industrial machinery and equipment manufacturing company with USD 54 million in revenue, 238 employees, and a stock symbol (6647) for a buy now price of USD 2,000. |
| **Access Sale** | An actor on a Russian language crime forum was selling access to multiple victims, including RDP access to a retailer in the drug store and pharmacies vertical with more than USD 720 million in revenue, an unnamed U.S. based hospital or clinic with more than USD 700 million in revenue, RDP access to a U.S. based CRM software developer with more than USD 520 million in revenue, and RDP access to a U.S. based building materials manufacturer. |
| **Access Sale** | An actor on a Russian language crime forum was selling access to an educational institution with USD 37.3 million in revenue. |
| **Access Sale** | An actor on a crime forum was selling access to a SQL database belonging to an unnamed U.S. based hospital or clinic with USD 74 million in revenue. |
| **Access Sale** | An actor on a crime forum is selling RDP access to a U.S. based business services management consulting company with USD 3.5 billion in revenue and 55,000 employees. |

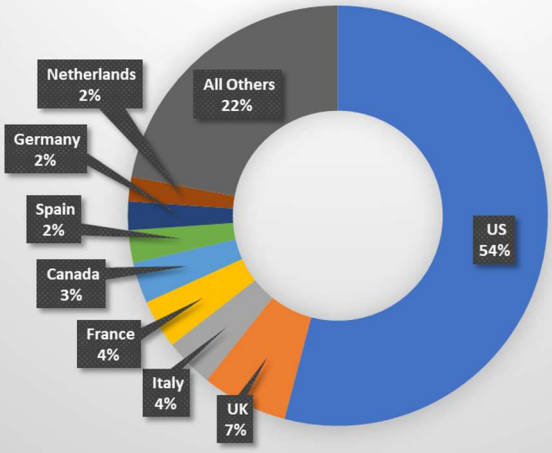
# By The Numbers

Summarizing incidents in graphical format

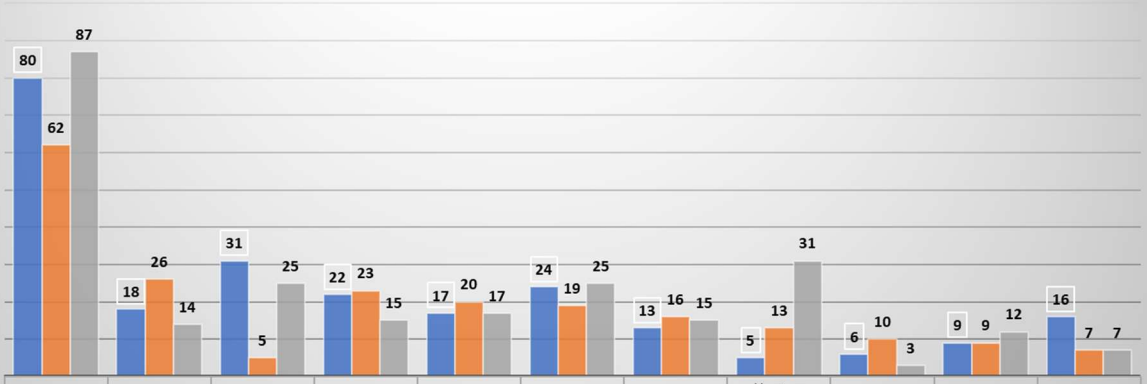


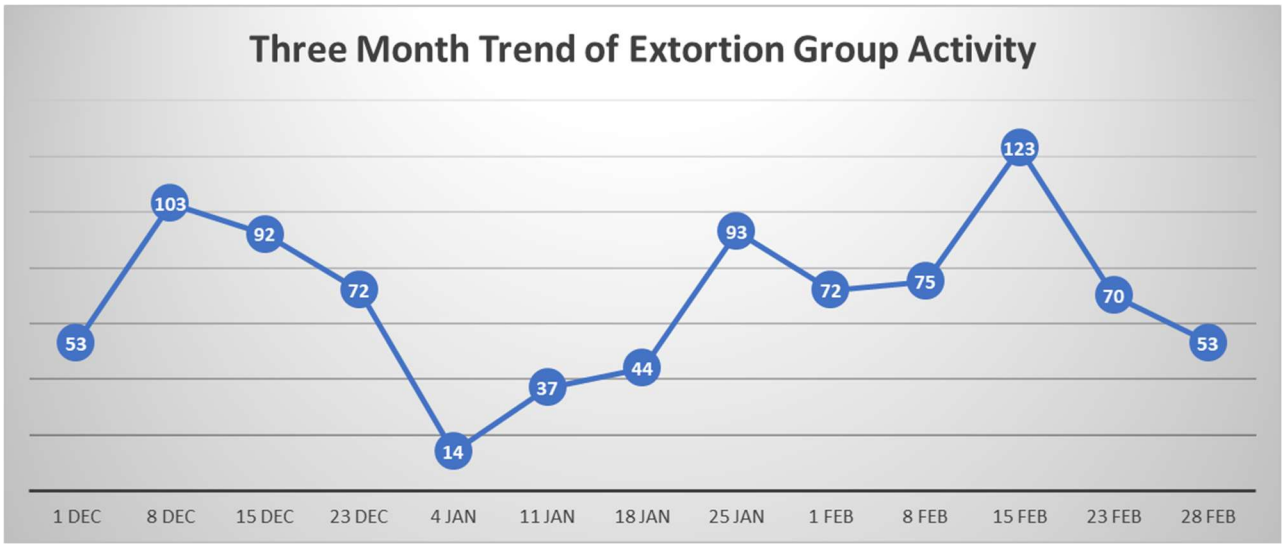
## Ransomware Victims By Country
## 318 Victims in 46 Countries




## Three Month Rolling Victims Count
## Selected Gangs



| | LockBit | Akira | Play | 8Base | Black Basta | Black Cat | BianLian | Hunters International | INC | Medusa | Cactus |
|---|---|---|---|---|---|---|---|---|---|---|---|
| December | 80 | 18 | 31 | 22 | 17 | 24 | 13 | 5 | 6 | 9 | 16 |
| January | 62 | 26 | 5 | 23 | 20 | 19 | 16 | 13 | 10 | 9 | 7 |
| February | 87 | 14 | 25 | 15 | 17 | 25 | 15 | 31 | 3 | 12 | 7 |


Three Month Trend of Extortion Group Activity
53
103
92
72
14
37
44
93
72
75
123
70
53
1 DEC
8 DEC
15 DEC
23 DEC
4 JAN
11 JAN
18 JAN
25 JAN
1 FEB
8 FEB
15 FEB
23 FEB
28 FEB

# New Detection Content

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

- **ConnectWise ScreenConnect Path Traversal Windows SACL**
  - This analytic detects attempts to exploit the ConnectWise ScreenConnect CVE-2024-1708 vulnerability utilizing Windows SACL EventCode 4663, which allows an attacker to perform path traversal attacks by manipulating the file_path and file_name parameters in the URL. The vulnerability, identified as critical with a CVSS score of 9.8, enables unauthorized users to access sensitive files and directories on the host system, potentially leading to the exfiltration of sensitive data or the execution of arbitrary code. The search query provided looks for file system events that could indicate exploitation attempts. This detection is crucial for identifying and responding to active exploitation of this vulnerability in environments running affected versions of ScreenConnect (23.9.7 and prior). It is recommended to update to version 23.9.8 or above immediately to remediate the issue, as detailed in the ConnectWise security advisory and further analyzed by Huntress researchers.

- **Confluence Pre-Auth RCE via OGNL Injection CVE-2023-22527**
  - This analytic identifies a critical template injection vulnerability (CVE-2023-22527) in outdated versions of Confluence Data Center and Server, which allows an unauthenticated attacker to execute arbitrary code remotely. The vulnerability is exploited by injecting OGNL (Object-Graph Navigation Language) expressions into the application, as evidenced by POST requests to the "/template/aui/text-inline.vm" endpoint with specific content types and payloads. The search looks for POST requests with HTTP status codes 200 or 202, which may indicate successful exploitation attempts. Immediate patching to the latest version of Confluence is strongly recommended, as there are no known workarounds. This detection is crucial for identifying and responding to potential RCE attacks, ensuring that affected Confluence instances are secured against this critical threat.

- **Windows SOAPHound Binary Execution**
  - The following analytic identifies the common command-line argument used by SOAPHound `soaphound.exe. ` Being the script is publicly available, function names may be modified, but these changes are dependent upon the operator. In most instances the defaults are used. It does not cover the entirety of every argument in order to avoid false positives.

- **Ivanti Connect Secure SSRF in SAML Component**
  - The following analytic is designed to identify POST request activities targeting specific endpoints known to be vulnerable to the SSRF issue (CVE-2024-21893) in Ivanti's products. It aggregates data from the Web data model, focusing on endpoints /dana-ws/saml20.ws, /dana-ws/saml.ws, /dana-ws/samlecp.ws, and /dana-na/auth/saml-logout.cgi. The query filters for POST requests that received a HTTP 200 OK response, indicating successful request execution.

- **Windows Privilege Escalation User Process Spawn System Process**
  - The following analytic detects when any process low->high integrity level process spawns a system integrity process from a user-controlled location. This behavior is often seen when attackers successfully escalate privileges to SYSTEM from a user-controlled process or service.

- **ConnectWise ScreenConnect Path Traversal**
  - This analytic detects attempts to exploit the ConnectWise ScreenConnect CVE-2024-1708 vulnerability, which allows an attacker to perform path traversal attacks by manipulating the file_path and file_name parameters in the URL. The vulnerability, identified as critical with a CVSS score of 9.8, enables unauthorized users to access sensitive files and directories on the host system, potentially leading to the exfiltration of sensitive data or the execution of arbitrary code. The search query provided looks for file system events that could indicate exploitation attempts. This detection is crucial for identifying and responding to active

exploitation of this vulnerability in environments running affected versions of ScreenConnect (23.9.7 and prior). It is recommended to update to version 23.9.8 or above immediately to remediate the issue, as detailed in the ConnectWise security advisory and further analyzed by Huntress researchers.

- **Windows Privilege Escalation System Process Without System Parent**
  - The following analytic detects any system integrity level process that was spawned by a process not running as a system account. This behavior is often seen when attackers successfully escalate privileges to SYSTEM from a user-controlled process or service.

- **Jenkins Arbitrary File Read CVE-2024-23897**
  - The following analytic identifies a Jenkins Arbitrary File Read CVE-2024-23897 exploitation. This attack allows an attacker to read arbitrary files on the Jenkins server. This can be used to obtain sensitive information such as credentials, private keys, and other sensitive information.

- **ConnectWise ScreenConnect Authentication Bypass**
  - This analytic detects attempts to exploit the ConnectWise ScreenConnect CVE-2024-1709 vulnerability, which allows an attacker to bypass authentication using an alternate path or channel. The vulnerability, identified as critical with a CVSS score of 10, enables unauthorized users to access the SetupWizard.aspx page on already-configured ScreenConnect instances, potentially leading to the creation of administrative users and remote code execution. The search query provided looks for web requests to the SetupWizard.aspx page that could indicate exploitation attempts. This detection is crucial for identifying and responding to active exploitation of this vulnerability in environments running affected versions of ScreenConnect (23.9.7 and prior). It is recommended to update to version 23.9.8 or above immediately to remediate the issue, as detailed in the ConnectWise security advisory and further analyzed by Huntress researchers.

[i] https://www.bleepingcomputer.com/news/security/trans-northern-pipelines-investigating-alphv-ransomware-attack-claims/
[ii] https://blog.bushidotoken.net/2024/02/lessons-from-isoon-leaks.html
[iii] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
[iv] https://cofense.com/blog/new-maas-infostealer-malware-campaign-targeting-oil-gas-sector/
[v] https://blog.talosintelligence.com/timbrestealer-campaign-targets-mexican-users/
[vi] https://twitter.com/rivitna2/status/1757053934852583891
[vii] https://www.orangecyberdefense.com/fileadmin/general/pdf/Ivanti_Connect_Secure_-_Journey_to_the_core_of_the_DSLog_backdoor.pdf
[viii] https://research.checkpoint.com/2024/raspberry-robin-keeps-riding-the-wave-of-endless-1-days/
[ix] https://medium.com/@DCSO_CyTec/to-russia-with-love-assessing-a-konni-backdoored-suspected-russian-consular-software-installer-ce618ea4b8f3
[x] https://lab52.io/blog/pelmeni-wrapper-new-wrapper-of-kazuar-turla-backdoor/
[xi] https://blog.morphisec.com/unveiling-uac-0184-the-remcos-rat-steganography-saga
[xii] https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
[xiii] https://www.fortiguard.com/psirt/FG-IR-24-015, https://www.fortinet.com/blog/psirt-blogs/importance-of-patching-an-analysis-of-the-exploitation-of-n-day-vulnerabilities