Monthly Threat Intelligence Rollup

DEEP seas

12/01/24-12/31/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
There Be Ransomware Over Yonder	A recent update published by supply chain management and SaaS provider Blue Yonder disclosed that the Termite ransomware gang has officially claimed responsibility for their November breach. This allowed Termite to acquire 680GB of data including database dumps, over 16,000 email addresses, and over 200,000 documents. What is most alarming about this attack is the reach - Blue Yonder has over 3,000 clients, including companies like Microsoft, Renault, Bayer, Tesco, Lenovo, DHL, 3M, Ace Hardware, Procter & Gamble, Carlsberg, Dole, Walgreens, Western Digital, and 7-Eleven. Many companies have already felt the ripple effects of this ransomware attack and took their systems offline, including a multinational chain of coffeehouses and roastery and two supermarket chains, who reportedly had to pay employees manually due to inoperable systems. The encryption software used in the attack was a version of the Babuk encryptor and not Termite's own encryptor, which is still a work in progress.[i] [ii]
Double Trouble for Critical Infrastructure	Cyble researchers have been monitoring two Russian hacktivist groups that are targeting critical infrastructure in the U.S., Canada, Australia, France, South Korea, Taiwan, Italy, Romania, Germany, Poland, and Ukraine. The two groups, Z-Pentest and People's Cyber Army, have also been sighted targeting different critical infrastructure supporting industries, with Z-Pentest going after oil facilities and People's Cyber Army looking for environmental cleanup and water systems companies. Z-Pentest has claimed 10 attacks since October, while People's Cyber Army has claimed eight. The two groups have also suggested they have a partnership, stating on the Z-Pentest Telegram that the Z-Pentest group thinks of People's Cyber Army as "comrades." Both groups also notably use screen recordings to prove unauthorized access to a victim's OT devices control systems, rather than screenshots.[iii]
LeakedData: New Threat on the Internet	In a recent article, Cyjax covered in detail a prolific extortion group calling themselves "LeakedData." LeakedData has claimed over 40 victims in the span of a month, with no indication currently on how the group managed to infiltrate these businesses. The group's victimology shows most of their attacks are against victims in the United States, with special attention given to the legal sector. Notably, independent security researchers have taken note of the group's sudden appearance and claim that the group could be fake. Their theory is that the group's true aim is to deliver the Ursnif banking Trojan to researchers navigating to their data leaks site in a watering-hole like attack.[iv]
Treasury Department Compromised by Suspected Chinese Nation-State Actors	According to Aditi Hardikar, the Assistant Secretary for Management at the U.S. Department of the Treasury, a recent breach at the Treasury has resulted in major implications. This December 8 attack was done by what is believed to be a China-based APT threat actor who remains unnamed. The breach was detected by their third-party software service provider, BeyondTrust, who explained to the Treasury that the unknown threat actor had somehow managed to access a key used by BeyondTrust to secure a cloud-based service that provides remote technical support for the Treasury Departmental Offices (DO) employees. Using this stolen key, the threat actor was able to bypass security and remotely access certain Treasury DO user workstations, therefore accessing classified documents, which is likely to be the attacker's main goal. To combat this threat, the Treasury has been collaborating with the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the intelligence community, and third-party forensic investigators to fully understand how the attack occurred and address impacted systems. The BeyondTrust service compromised by the attackers has also been taken offline and no longer has access to internal Treasury data.[v]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
A Clever Way to Get in Trouble	Rapid7 Labs has found a novel malware installer called “CleverSoar,” which was developed to evade detection and deploy the Winos4.0 framework, the Nidhogg rootkit, and a custom backdoor for exfiltration.	Although the threat actor behind creating this installer is currently unknown, their target victims are clear. The actor is looking only for Chinese or Vietnamese potential victims and is terminating installation if the victim’s device does not use either language. Because of this direct targeting, it can be inferred that the unknown group is likely a cyber criminal organization and performing these attacks for financial gain. The attack chain for CleverSoar starts with an MSI installer that drops CleverSoar and all later malwares. CleverSoar is then executed and runs various anti-sandbox and anti-debugging checks, along with the aforementioned language check, and if any of these checks fail, the infection is stopped. If the checks pass, a vulnerable sysmon driver (tProtect.dll) is exploited to execute at system startup and utilized to disable security software. Nidhogg is then set to run on startup, and both Winos4.0 and the custom backdoor are executed and used immediately by the attackers.[vi]
Activating Infection in a Hands-On Manner	Kaspersky has unearthed a new method for delivering RedLine stealer via a weaponized version of the HPDxLIB activator software.	Infection occurs when the victim is coerced into replacing techsys.dll with the version provided by the fake activator. When the activator is launched, a legitimate process labeled 1cv8.exe loads the malicious library, which then launches the stealer. These attacks were targeted toward Russian-speaking entrepreneurs and businesses who may use software to automate business processes and want to save money using an activator, however illegal that may be. It is also important to mention that this attack can only occur due to social engineering, as they do not exploit any vulnerabilities to gain access.[vii]
DarkNimbus Clouds the Sky	Trend Micro researchers have pieced together an Earth Minotaur campaign pushing a new backdoor labelled as “DarkNimbus.”	This backdoor is delivered using the MOONSHINE exploit kit to deliver the backdoor to both Android and Windows devices. The attack starts with Earth Minotaur generating links from MOONSHINE that are used later in instant messaging chats to get victims to go to the link and download MOONSHINE. Victims are then instructed to download DarkNimbus to a victim’s device, where DarkNimbus then connects to the Earth Minotaur C2 where attackers can interact with DarkNimbus. DarkNimbus contains a vast number of features, including information gathering on the infected device, any installed apps, and the device’s geolocation. From these locations, the backdoor can steal data such as contact lists, phone call records, SMS content, clipboard content, browser bookmarks, and conversation IM applications such as Skype, WhatsApp, WeChat, and more. It also supports call recording, photo capturing, screenshotting, modifying files, and executing commands remotely.[viii]

Loading Up New Upgrades	Zscaler ThreatLabz has continued to follow the development of Zloader by various adversaries.	These changes have three key points. The first is that the newest version of Zloader (2.9.4.0) has made noteworthy improvements to its C2 communication, deploying a custom DNS tunnel protocol, along with an interactive shell that supports more than a dozen commands, such as running DLL files from memory, finding processes by name or PID, terminating processes, and more. Second, the trojan now comes with new anti-analysis techniques, such as environment checks to determine if a victim device is worth pursuing further and API import resolution algorithms to evade detection from sandboxing and static signatures. Finally, a change in methodology of how to perform initial infection has been employed, with the Zloader threat actor social engineering a victim into installing RMM software such as AnyDesk, TeamViewer, and Microsoft Quick Assist for easy remote sessions.[ix]
Careto Actor Returns After Long Hiatus	Kaspersky researchers have identified a campaign operated by the Careto threat actor, also known as “The Mask,” who has not been seen operating in the wild in several years.	The identified campaign starts with a MDaemon email server being compromised, along with further persistence being applied by using a MDaemon webmail component, called WorldClient, which allows for extensions to be loaded that handle the custom HTTP requests from clients to the email server. Careto then uses their own, custom extension to interact with the email server through HTTP requests. This extension is then used to gather information about the infected organization and spread it to other computers inside its network. The main goal of the campaign is to install “FakeHMP,” a novel implant that can retrieve files, log keystrokes, take screenshots, and deploy further payloads to infected machines.[x]
A Very Bad Kitty Dropping PUMA Rootkit	Elastic Security Labs found a new evasive LKM rootkit through VirusTotal hunting, named by its authors as “PUMA” and known by Elastic as “PUMAKIT.”	The infection chain for the malware begins with an ELF dropper named “cron” that checks the command line for the keyword argument "Huinder" before continuing. If the check is successful, cron delivers the next stage. This consists of two executables stored in memory, “/memfd:tgt,” a legitimate cron binary likely used for decoy purposes, and “/memfd:wpn,” which is the loader for PUMAKIT. Before the loader executes, however, further checks are made for attacker complications like secure boot. If successful, a shell script is run which then installs the rootkit. Following this, a shared object called “Kitsune” is also employed and facilitates the persistence and stealth mechanisms of PUMAKIT.[xi]
Losing CONTROL	Team82 obtained and analyzed a new piece of IoT and OT malware made by the Iranian threat group CyberAv3ngers called “IOCONTROL.”	IOCONTROL is an IoT and OT malware framework for targeting Linux that can be customized for different use cases. This customization is important due to the sheer amount of IoT and OT devices used today, such as IP cameras, routers, PLCs, HMIs, firewalls, and more. It supports commands such as code execution, artifact removal, port scanning, and more. IOCONTROL also has a persistence mechanism and stealth mechanisms, for example using DNS over HTTPS to hide C2 communication. Thus far, IOCONTROL has been observed being used to target enemies of Iran, such as fuel management companies in the U.S. and Israel.[xii]
Winnti Group Proves to be Data Gluttons	XLab has brought to light a previously undocumented advanced PHP backdoor dubbed	This backdoor has been used to target industries such as IT services, business operations, and social security in the U.S. and China. Glutton can retrieve system information and the Baota Linux Panel data used for server management, including

	"Glutton" and linked it to the Chinese nation-state Winnti Group.	credentials and management interface details. The backdoor is believed to be spread through exploiting vulnerabilities, brute-forcing passwords, and infecting other threat actors to gain a foothold into their successful breaches. Glutton shows many developmental downfalls, however, such as a lack of C2 encryption, using HTTP instead of HTTPS for downloads, and no obfuscation to the code at all.[xiii]
Cybercriminal Crafts a VIP (Very Invasive Program) Malware	ForcePoint has announced their discovery of a novel information stealer labelled as "VIPKeyLogger."	The attack chain is par for the course of malware these days, with a malicious Microsoft Word file sent to the victims through phishing emails. The Word file, after enabling macros, downloads VIPKeyLogger, and the malware begins operation. Some of the data collected includes device names, country location, clipboard data, screenshots, cookies, bowser history, and more. The stealer then sends collected data to the attacker's C2 through Telegram to Dynamic DuckDNS servers.[xiv]
The Arrival of a Data Demon	The Netskope team has dug up an unknown backdoor tied to the iTop Data Recovery application that the group has named "Yokai."	While initial means of infection has not been confirmed, a RAR file was detected through Netskope hunting activities that contained two LNK files. One file was simply a PDF decoy; the other, however, had another decoy DOCX document with an embedded dropper executable. This dropper then left a legitimate copy of the iTop Data Recovery application on the victim's device, along with side-loading Yokai backdoor. With Yokai, attackers can execute commands, maintain persistence, and communicate with their C2 servers.[xv]
Another Stealer in the Shadows	Morphisec has made note of a previously undocumented information stealer called "CoinLurker."	While the malware does have cryptocurrency stealing functionality, it also can target financial applications and other programs such as Telegram Desktop, tdata, Discord, Local Storage, leveldb, and FileZilla. Its goal targeting this software is to steal any useful credentials. CoinLurker has been seen delivered through many avenues, including fake software update notifications, malvertising redirects, phishing emails, fake CAPTCHA prompts, direct downloads from fake or compromised sites, social media, and messaging links. The stealer has also been seen implementing EtherHiding to conceal payloads by embedding the payload into a Binance Smart Contract, which communicates with the attacker's C2 and downloads CoinLurker from an attacker controlled Bitbucket repository.[xvi]
A Bitter End to the Year	Proofpoint has identified a new line of TTPs associated with the India-based threat group known as "Bitter."	These new TTPs can be explained best by observing the infection chain, with Bitter first sending the victim a spear phishing email. Within this email is a RAR file that contains an LNK file disguised as a PDF, a hidden malicious PDF ("~tmp.pdf"), and two hidden Alternate Data Stream (ADS) files ("Zone.Identifier" and "Participation"). To start, the Zone.Identifier stream is an established part of the Windows NT File System (NTFS) and is used in this case passively to change the URL Security Zone of the files downloaded from the phishing email to another zone deemed more trustworthy, such as Local Machine or Trusted Sites. Being the only visible file to the victim, when clicked the LNK runs the command "--headless cmd /k "cmd < ~tmp.pdf:Participation & exit" in conhost, which calls on ~tmp.pdf to run hidden PowerShell within the Participation ADS stream, whereafter a decoy PDF is

		shown to the victim to throw them off, along with a scheduled task that attempts to exfiltrate data on the victim's device to an attacker controlled domain. After receiving the data, Bitter then infects the victim with WmRAT, MiyaRAT, or both. So far, there is only one documented victim, a defense sector organization in Turkey.[xvii]
The Siemens Killer: Chaya_003	Forescout Research has identified a malware cluster used to terminate Siemens TIA portal processes, which Forescout has named "Chaya_003."	Chaya_003 is believed to be created by the previously undocumented Belgian threat groups "h921 industries," "x86assembly.xyz" and "Team WhoStoleMyComputer." It is used to exfiltrate data and stop certain processes related to Siemens "Totally Integrated Automation Portal," or TIA Portal, which allows users to design and manage automation systems. The malware uses Discord webhooks for C2 communication and send commands through curl. Using the CreateToolhelp32Snapshot Win32 API call, system processes are then itemized. Following this, the Process32First function is called, allowing Chaya_003 to collect victim data about each process and compares recognized software to a predefined list of applications to be terminated, consisting of "word.exe," "excel.exe," "code.exe," "powerpnt.exe," "teams.exe," "chrome.exe," "firefox.exe," "Siemens.Automation.Portal.exe," and "PakcetTracer.exe."[xviii]
Out of the Ashes	Qualys threat researchers have found a new strain of ransomware titled "NotLockBit," which can target macOS and Linux systems.	The execution chain of the ransomware is explained by Qualys as starting with the use of the go-sysinfo module to gather system information. The public key encrypted in the Privacy Enhanced Mail (PEM) file is then decoded and used to generate and encrypt a private key. All collected data and keys are then stored in a text file. AWS is used for data exfiltration, with the attacker's AWS credentials being hardcoded into NotLockBit. The process of encryption is then begun, encrypting by common or sought after file extensions and avoiding certain directories. To make sure the victim is aware of infection, NotLockBit changes the victim's desktop background to be their ransom note. And finally, after the wallpaper is altered, NotLockBit begins its self-deletion, along with deleting any shadow copies.[xix]
Anonymous Communications Abused Again	X user @Gi7w0rm has uncovered a new RAT that abuses the I2P Anonymous Network which is rightly named "I2PRAT."	The infection chain of this new malware starts when a phishing email with a malicious link embedded is sent to the victim. This link contains a fake captcha, which secretly copies a PowerShell script to the clipboard and tricks the victim into pasting it onto their device. This script pulls down a loader that uses native APIs and employs a UAC bypass technique to elevate its status. After running with higher privileges, the loader decrypts and reflectively loads a payload. This payload performs many actions, such as using I2P for encrypted C2 communication, along with dropping further files and RATs. These further files have abilities such as manipulating Windows Defender settings and blocking certain traffic using Windows Filtering Platform.[xx]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
The Argonauts' Attempt to Pull the Wool Over Our Eyes	Cyjax has uncovered a new extortion group going public as the "Argonauts Group." According to Cyjax, the Argonauts Group has claimed 10 victims so far, mainly healthcare-related organizations in either Italy, Taiwan, or Japan. Notably, if victims do not pay, the Argonauts Group is not shy to post stolen data. In two such cases where payment was refused to the Argonauts Group, 200GB and 140GB of PII, internal documents, and more were taken from each business and posted for free on their Argonauts Group DLS. Because their "Sold" page is empty, it can be assumed that the group has not seen any rewards for their efforts, but due to the group's newness, it remains to be seen whether the group will be respected in the cyber criminal space.[xxi]
Earth Kasha Goes Old School	Rapid7 Labs Trend Micro has noted a recent shift in campaign strategy from the Chinese threat group, Earth Kasha. Their most recent campaign does away with their new strategy of targeting edge devices and returns to form by employing spear phishing campaigns. This newest campaign also has the end goal of delivering the ANEL backdoor to its victims, rather than the groups prior use of LODEINFO and NOOPDOOR. The phishing emails received came with a OneDrive link containing a ZIP file which contains Earth Kasha interchanges based on the details of the victim. The three recorded ways Earth Kasha does this are through either a macro-enabled document, a shortcut file and an SFX, or a shortcut file that drops a CAB file. Some additional new malware spotted was "ROAMINGMOUSE," a dropper, and "ANELLDR," a loader.[xxii]
A New Sting with a Howling Pain	Unit 42 researchers have noticed a change in tools and malware from the Howling Scorpius ransomware group, known for the development and use of Akira ransomware. These changes include both encryptors from Windows, Linux, and ESXi devices, along with an updated toolset using tools such as EDRSandBlast, Mimikatz, Rclone, PsExec, and Cobalt Strike. Regarding the encryptors, the Windows variant uses ChaCha20 algorithm for encryption, can delete shadow copies, and can customize how far they wish to encrypt a victim's file through commands such as controlling the amount of data to be encrypted within each file and preventing remote drive encryption. Similarly, the Linux and ESXi variants can control how far to take encryption, but also can disable logging and the Core Dump file.[xxiii]
All for One	Microsoft Threat Intelligence recently published new research on the Russian nation-state actor tracked by Microsoft as Secret Blizzard, known more commonly as the Turla APT group, and their use of other threat actors' tools and infrastructure. In terms of infrastructure, Turla has been seen compromising the C2s of the Pakistan-based espionage group labelled as Storm-0156, as well as using their backdoors. Regarding tools, Turla has been seen using Storm-0156's C2 tool Arsenal, CrimsonRAT, and Wainscot. Turla's need in commandeering Storm-0156's tools and infrastructure comes from their goal of installing backdoors and collecting intelligence on targets of interest in South Asia, as Turla is known for committing espionage.[xxiv]
Free Trial Used for Free Evasion Detection	Insikt Group researchers have determined that the state-sponsored threat group BlueAlpha has updated their malware delivery chain to utilize Cloudflare tunnels to transport GammaDrop malware to victim devices. This is done by abusing the TryCloudflare tool, which allows anyone to create a tunnel using a randomly generated subdomain of "trycloudflare.com" and subsequently have all requests to that subdomain be proxied through Cloudflare's infrastructure. As a further incentive, TryCloudflare is a free trial tool, meaning that attackers do not even need to pay to use its services. BlueAlpha uses this tunneling service to conceal staging infrastructure used to deploy GammaDrop and to evade network detection. A malicious LNK file is delivered to the

	victim through these tunnels containing GammaDrop for infection.[xxv]
Black Basta's New Plan	Rapid7 has observed a change in the TTP of the Black Basta ransomware group. Their campaign now features new malware payloads, such as Zbot, DarkGate, Cobalt Strike, and other custom-made tools. Delivery methods have also evolved, with Black Basta either bombing victims with phishing emails containing malicious attachments, employing Microsoft Teams social engineering, or exploiting vulnerabilities in software. In cases of successful social engineering, Black Basta will instead install a RMM tool onto the victim's device for remote control capabilities. New defense evasion tactics include the use of obfuscated scripts, disabling security software, and leveraging legitimate tools like PowerShell for malicious purposes.[xxvi]
Opening the Digital Eye	Tinexta Cyber and SentinelLabs has pieced together evidence to show proof of a new campaign believed to be run by an unnamed Chinese state-sponsored APT group. This campaign, named "Operation Digital Eye," was seen targeting business-to-business IT service providers in Southern Europe. The campaign starts with a SQL injection into an internet-facing web or database server. Next, a PHP webshell is deployed to establish a foothold and maintain persistence. Reconnaissance is then done using third-party tools and built-in Windows utilities and credentials are stolen using CreateDump. RDP, along with pass-the-hash techniques, are used to move laterally on the network. The most interesting part, however, is the threat actors leveraging Visual Studio Code Tunnels for remote code execution. These tunnels provide full endpoint access, including command execution and filesystem manipulation. Visual Studio Code tunneling also functions on signed Microsoft executables which can go under the radar and are typically allowed by application controls and firewalls.[xxvii]
Hunting Down Our Nemeses	Independent researchers have shed light on a new campaign facilitated by the actions of two threat groups, "Nemesis" and "ShinyHunters." The researchers described the campaign as two parts - discovery and exploitation. Discovery first begins with the attackers obtaining a list of publicly available AWS IP address ranges consisting of long lists of CIDRs (Classless Inter-Domain Routing). Next, using open-source tools, the attackers expanded the CIDRs into extensive lists of IP addresses where Shodan was used to reverse lookup the AWS IP addresses to acquire the IP's domain name. Based on the hosts found in discovery, various tests are performed on them to determine the best way to extract data. Some of the data sought after by the attackers include AWS customer keys and secrets, Git credentials and source code, Twillio, Vonage, and Exotel keys, along with credentials for databases, SMTP, CPanel, SSH, Sendgrid, Google accounts, Facebook, OneSignal, ToxBox, Plivo, and more. The groups also attempted to gain access to various AWS services such as the IAM, SES, SNS, and S3 buckets.[xxviii]
A New Mysterious, Unattributed Threat	Datadog Security Labs threat research has found a new threat actor, identified by Datadog as "MUT-1244." While not much is known about the group itself, their methodology has been thoroughly documented. For initial access, MUT-1244 uses two vectors to compromise their victims, either through spear phishing or by trojanizing GitHub repositories. The second stage of attack is the use of "xmrdropper," which contains a cryptocurrency miner and a backdoor that exfiltrates system data, SSH keys, AWS keys, environment variables, and any files of interest to the group on the affected device to the file sharing service file.io. So far, over 390,000 WordPress account credentials have been stolen through the group's trojanized "yawpp" GitHub project alone, which tricks visitors by masking as a WordPress credentials checker. Documented victims include not only penetration testers and security researchers, but other threat actors as well.[xxix]
No Stops on the RAT Train	The Federal Bureau of Investigation (FBI) exposed a campaign targeting IoT devices in the U.S., UK, Australia, Canada, and New Zealand with HiatusRAT. To find potential victims, the attackers used a webcam scanning tool titled as "Ingram" to scan for vulnerable web cameras and DVRs within these countries that are known for

	vulnerabilities such as CVE-2017-7921, CVE-2018-9995, CVE-2020-25078, CVE-2021-33044, CVE-2021-36260, along with checking for weak passwords. Devices were also targeting based on brand; for example, Xiongmai and Hikvision devices with telnet access were especially targeted. After a victim has been found, the attackers then used Medusa to brute-force the authentication process. Once in the environment, HaitusRAT is deployed into the victim's environment.[xxx]
The Scoundrels of the Russian Federation	Trend Micro's global threat intelligence has explained well in their recent research the changes in methodology of the Russian state-sponsored threat group, APT29. Specifically, Trend Micro emphasized APT29's use of rogue RDP attacks, which leverages a RDP relay, a rogue RDP server, and a malicious RDP configuration file to potentially allow the group to access files, plant malware, and execute remote code. The initial infection is delivered through spear-phishing emails that try to convince possible victims to run the RDP configuration file, causing their machines to connect to one of the group's 193 RDP relays and beginning the attack. These emails were sent to industries such as government bodies, military, think tanks, academic researchers, and miscellaneous Ukrainian targets. Notably, to minimize detection, APT29 uses a man-in-the-middle proxy in front of the RDP servers and uses a Python tool called "PyRDP," which captures traffic, credentials, sessions, and clipboard data, along with relaying data to and from the server and victim, in addition to data modification and injection capabilities.[xxxi]
Cloud Atlas' New Cloud Malware Suite	Kaspersky has stated clearly that the Russian threat group Cloud Atlas has been seen using new tools in its attacks, going by the titles of "VBCloud," "VBShower," and "PowerShower." VBCloud is the main payload and is a backdoor that uses cloud services for C2 communication, because cloud-based C2 channels are more challenging to detect. VBShower, however, is used as a cleanup tool to delete leftover artifacts of their attacks to minimize the chances of detection. Finally, there is PowerShower, which is a PowerShell-based tool used to execute malicious commands and scripts on compromised systems, facilitating the various stages of their Cloud Atlas' attack chain, including reconnaissance, payload deployment, and data exfiltration. According to Kaspersky, 82% of Cloud Atlas victims were in Russia, with other attacks taking place in Belarus, Canada, Moldova, Israel, Kyrgyzstan, Vietnam, and Turkey.[xxxii]

Dark Web Markets

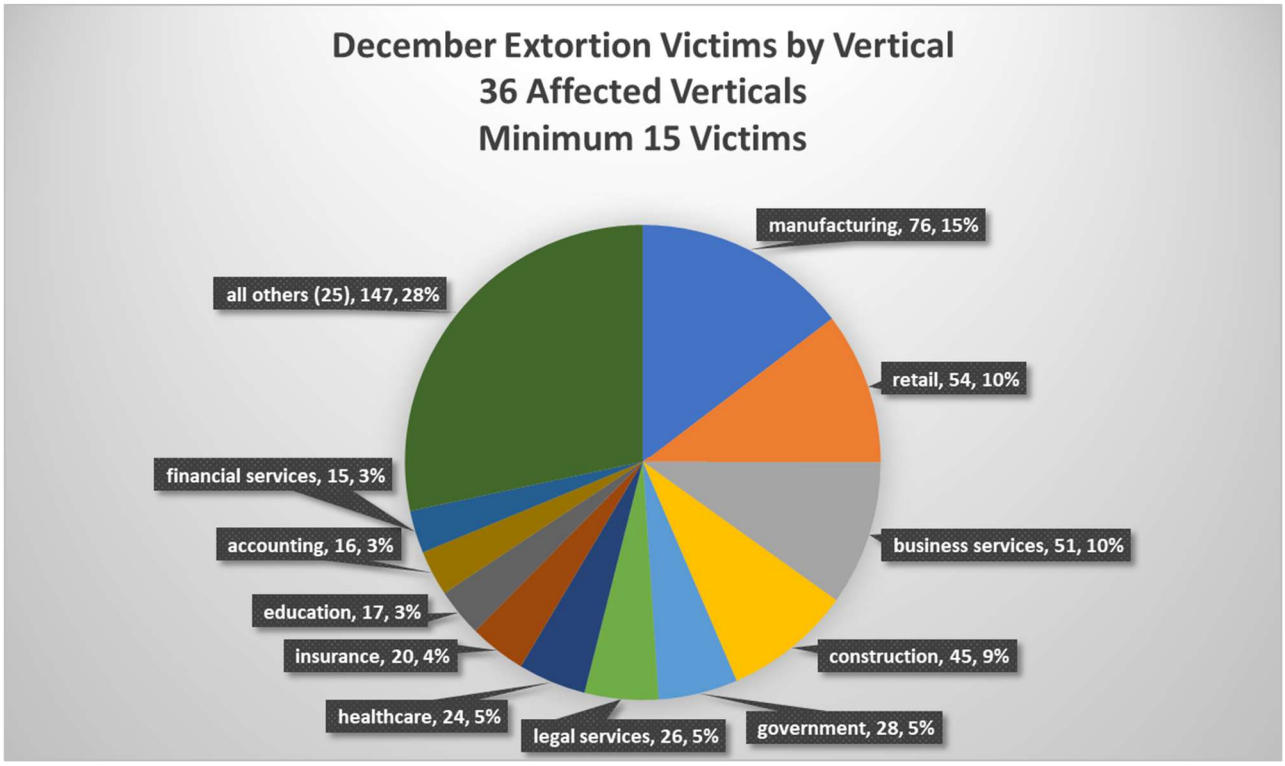
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

Activity	Note
Access Sale	An actor was observed selling Palo Alto Global Protect access to a U.S.-based insurance company with between USD 35-40 billion in revenue for USD 25,000. In response to queries, the actor claimed the company has more than 30,000 employees and that they only have user creds.
Access Sale	An actor was observed selling RDWeb access to a U.S.-based commercial and residential construction company with 266 employees and USD 40.7 million in revenue for USD 2,500.
Actor Developments	An actor who leads a criminal penetration test team – a crime forum euphemism for ransomware affiliate team – is looking for initial accesses in the accounting and legal services verticals in Australia, Canada, the U.S., and E.U. The price for initial accesses starts at USD 1,000, and they are offering up to 25% of the ransom for a successful breach.
Actor Developments	DragonForce team announced an update to their ransomware on a popular crime forum. The most important change was support for attacks on ESXi 5.5.
Tool Sale	A new actor was observed selling what they claim is "multiple full chain Palo Alto exploits resulting in RCE." They were asking USD 5,000 and did not further describe the exploit, although there have been several high-profile Palo Alto vulnerabilities disclosed recently.
Access Sale	An actor was observed selling what they claimed was 1,676,292,554 Gmail accounts in mail:pass format for a buy now price of USD 800. If this dubious claim is true, this would represent 90% of all Gmail accounts in existence.
Access Sale	An actor was observed selling RDP access to a Swedish transportation company with more than USD 1.7 billion in revenue for USD 1,000.
Access Sale	A new actor was observed selling VPN access to multiple victims, including a tire manufacturer with USD 2.9 billion in revenue and an enterprise in the construction vertical with USD 658.9 million in revenue.
Access Sale	An actor was observed selling domain admin access to a Canadian television broadcaster with USD 120 million in revenue for USD 15,000.
Actor Developments	More than six months after being disrupted by law enforcement, the actor who sold Smoke Loader malware has resurrected the brand with what they claimed is an improved version with additional features. They are only selling one license for USD 2,000/week.
Access Sale	An actor was observed selling L3 VPN access to an unidentified car rental agency with more than USD 100 million in revenue and more than 900 hosts in two domains for USD 700.
Access Sale	An actor reportedly sold domain admin access to a company described as a “technological defense company” with USD 22 million in revenue for USD 7,000.
Access Sale	An actor was observed selling Fortinet domain user access to a human resources and staffing company with USD 550.1 million in revenue for USD 1,500

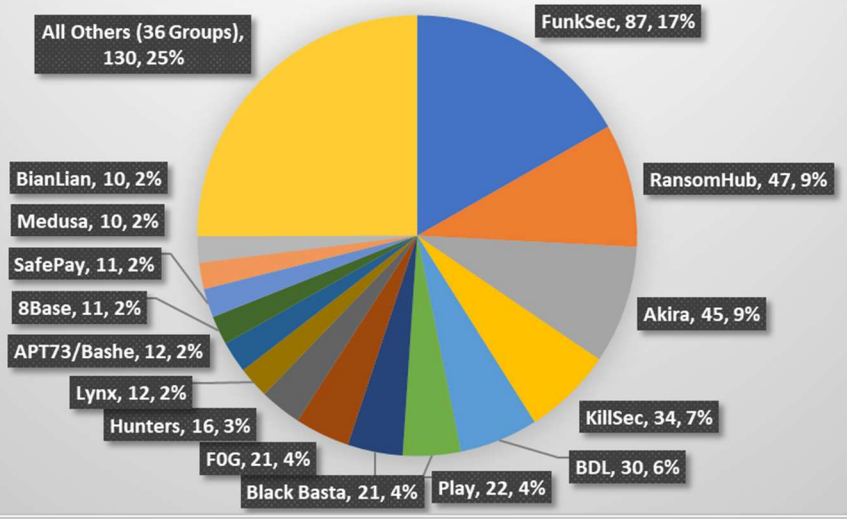
Access Sale	An access seller was observed selling full Microsoft 365 access to an unidentified oil and gas company in an unidentified Arabic speaking country with USD 197.5 million in revenue for USD 1,600. He claimed there is access to emails with a legal perspective and details on business deals.
Data Sale	An actor was observed attempting to sell more than 700,000 lines of medical data/PHI taken from Minnesota based CentraCare. This data was likely from last year's MoveIT breach by Cl0p ransomware.
Access Sale	An actor was observed selling AnyDesk local admin access to a U.S.-based grocery retailer with USD 1 billion in revenue for USD 12,000. A known ransomware actor made an opening bid of USD 8,000 for the access.
Access Sale	An actor was observed selling Jenkins and AWS access to a U.S.-based fintech company with more than USD 1.5 trillion in assets under management for USD 9,500.
Data Sale	An actor was observed selling what he claimed was 30 GB of confidential data from Qatar Gas, ADNOC, and Bell Energy. He did not describe how he obtained this data.
Data Sale	A crime forum moderator was observed selling more than 66,000 rows of customer data stolen during an alleged December 2024 breach of motorcycle maker Harley Davidson.

By The Numbers

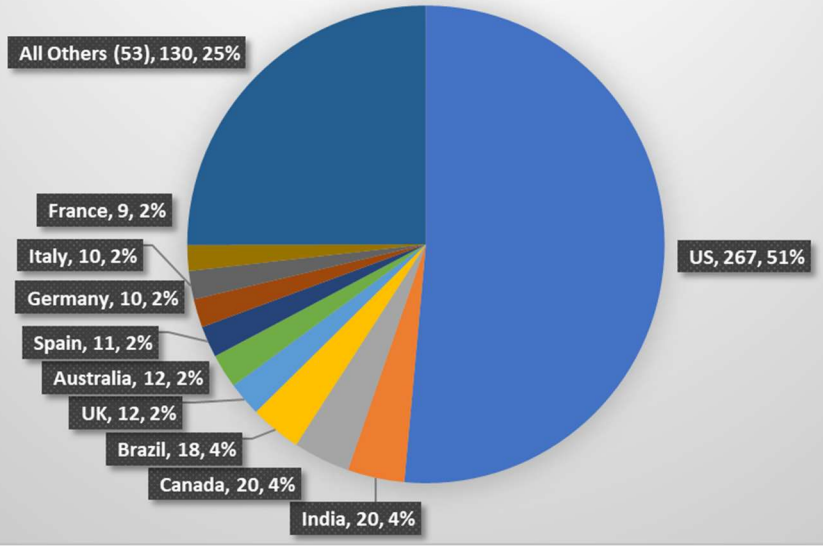
Summarizing incidents in graphical format

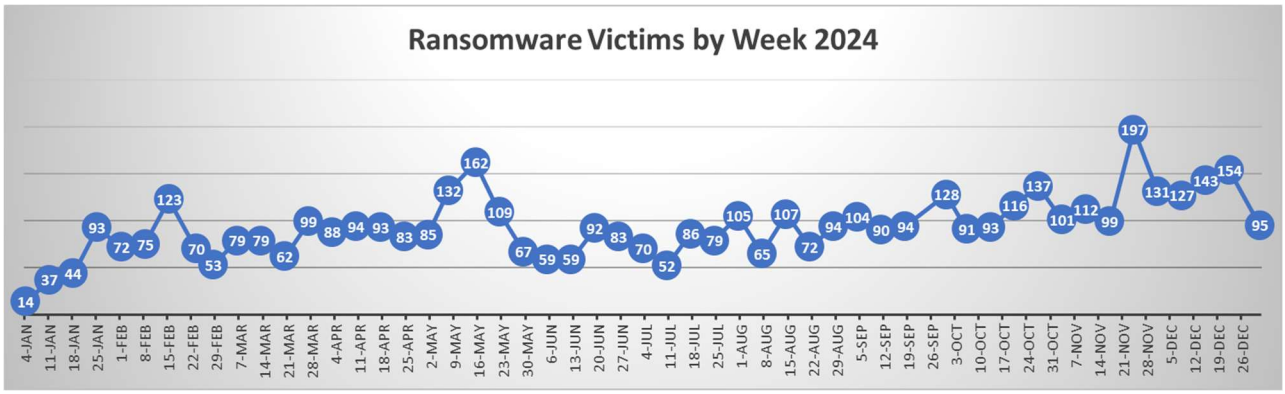


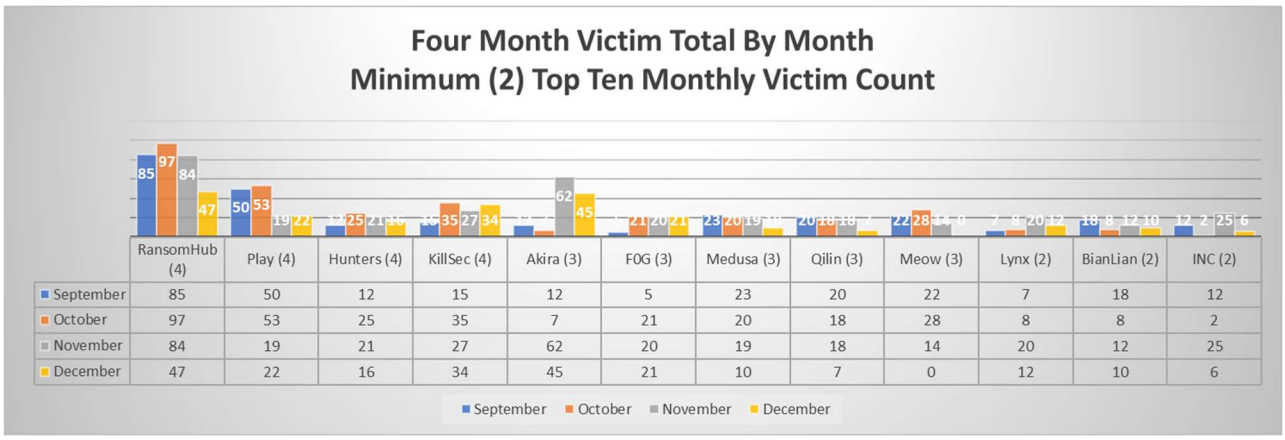
December Extortion Victims by Group
51 Active Groups
Minimum 10 Victims
519 Total Victims



December Extortion Victims by Country
63 Total Countries
Minimum 9 Victims







	RansomHub (4)	Play (4)	Hunters (4)	KillSec (4)	Akira (3)	FOG (3)	Medusa (3)	Qilin (3)	Meow (3)	Lynx (2)	BianLian (2)	INC (2)
September	85	50	12	15	12	5	23	20	22	7	18	12
October	97	53	25	35	7	21	20	18	28	8	8	2
November	84	19	21	27	62	20	19	18	14	20	12	25
December	47	22	16	34	45	21	10	7	0	12	10	6

New Detection Content

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

- **Cleo Transfer Software Exploit**
    a. Cleo has identified an unrestricted file upload and download vulnerability (CVE-2024-50623) that could lead to remote code execution.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
    c. **Source**: https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild
- **Sqlcmd Targeting Veeambackup**
    a. Detects attempts to retrieve credentials from VeeamDatabase
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
- **XenArmor Password Recovery Tools**
    a. XenArmor is a commercial product that can retrieve keys from local computers, external disks, registry hive files, and even remote computers on the same network. However, it can be used maliciously as a credential and info-stealer.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
    c. **Source**: https://xenarmor.com/
- **VSCode Dev Tunnel Usage**
    a. The tunnel parameter instructs Visual Studio Code to create a dev tunnel and act as a server to which remote users can connect. After authenticating to the tunnel with a Microsoft or GitHub account, remote users can access the endpoint running the Visual Studio Code server, either through the Visual Studio Code desktop application or the browser-based version, vscode.dev.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
    c. **Source**: https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/
- **Schtasks With Interpreter Command**
    a. Detects scheduled tasks being loaded with a one-liner payload.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
- **Quick Assist Remote Tool**
    a. Per Microsoft - "Threat actors misuse Quick Assist features to perform social engineering attacks by pretending, for example, to be a trusted contact like Microsoft technical support or an IT professional from the target user's company to gain initial access to a target device." It should be checked if this is approved software.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
    c. **Source**: https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

- **Createdump Tool Usage**
    a. Microsoft .NET Runtime Crash Dump Generator (included in .NET Core). This can be used to target the lsass process.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
    c. **Source**: https://lolbas-project.github.io/lolbas/OtherMSBinaries/Createdump/
- **Remote Utilities RAT**
    a. Remote access tool "Remote Utilities," also known as RURAT has been utilized by threat actors to access systems.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
    c. **Source**: https://redcanary.com/blog/threat-detection/misbehaving-rats/
- **Processes Running from Uncommon Directories**
    a. Detects malware running from uncommon locations.
    b. **Platforms**: CarbonBlack, SentinelOne, Defender, CrowdStrike
    c. **Source**: https://www.bitdefender.com/en-us/blog/labs/luminousmoth-plugx-file-exfiltration-and-persistence-revisited

---

[i] https://www.bleepingcomputer.com/news/security/blue-yonder-saas-giant-breached-by-termite-ransomware-gang/
[ii] https://blueyonder.com/customer-update
[iii] https://cyble.com/blog/russian-hacktivists-target-energy-and-water-infrastructure/
[iv] https://www.cyjax.com/resources/blog/alleged-extortion-group-leakeddata-begins-to-leak-data/
[v] https://legacy.www.documentcloud.org/documents/25472740-letter-to-chairman-brown-and-ranking-member-scott/
[vi] https://www.rapid7.com/blog/post/2024/11/27/new-cleversoar-installer-targets-chinese-and-vietnamese-users/
[vii] https://securelist.ru/redline-stealer-in-activators-for-business-software/111241/
[viii] https://www.trendmicro.com/en_us/research/24/l/earth-minotaur.html
[ix] https://www.zscaler.com/blogs/security-research/inside-zloader-s-latest-trick-dns-tunneling
[x] https://securelist.com/careto-is-back/114942/
[xi] https://www.elastic.co/security-labs/declawing-pumakit
[xii] https://claroty.com/team82/research/inside-a-new-ot-iot-cyber-weapon-iocontrol
[xiii] https://blog.xlab.qianxin.com/glutton_stealthily_targets_mainstream_php_frameworks-en/#analysis-of-glutton
[xiv] https://www.forcepoint.com/blog/x-labs/vipkeylogger-infostealer-malware
[xv] https://www.netskope.com/blog/new-yokai-side-loaded-backdoor-targets-thai-officials
[xvi] https://blog.morphisec.com/coinlurker-the-stealer-powering-the-next-generation-of-fake-updates
[xvii] https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-chain-delivers-espionage-rats
[xviii] https://www.forescout.com/blog/ics-threat-analysis-new-experimental-malware-can-kill-engineering-processes/
[xix] https://blog.qualys.com/vulnerabilities-threat-research/2024/12/18/notlockbit-a-deep-dive-into-the-new-ransomware-threat
[xx] https://www.gdatasoftware.com/blog/2024/12/38093-ip2rat-malware
[xxi] https://www.cyjax.com/resources/blog/new-argonauts-extortion-group-emerges/
[xxii] https://www.trendmicro.com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign.html
[xxiii] https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/
[xxiv] https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/
[xxv] https://go.recordedfuture.com/hubfs/reports/cta-ru-2024-1205.pdf
[xxvi] https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/

[xxvii] https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/
[xxviii] https://www.vpnmentor.com/news/shiny-nemesis-report/
[xxix] https://securitylabs.datadoghq.com/articles/mut-1244-targeting-offensive-actors
[xxx] https://www.ic3.gov/CSA/2024/241216.pdf
[xxxi] https://www.trendmicro.com/en_no/research/24/l/earth-koshchei.html
[xxxii] https://securelist.com/cloud-atlas-attacks-with-new-backdoor-vbcloud/115103/