Monthly Threat Intelligence Rollup

DEEP seas

11/01/24-11/30/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Keep Your Data Under Lock and Key	The Cisco Talos Incident Response team recently detected activity from the Interlock cyber criminal ransomware group. Their newest attack chain starts with a fake Google Chrome browser update downloaded from a compromised website. The downloaded executable is a RAT which installs Chrome as a decoy and sets itself in the Windows startup folder for persistence. The unnamed RAT then collects system information, encrypts said data, and sends it to the attacker's C2. After this, further malware is downloaded, such as a credential stealer and a keylogger. Once inside, the Interlock group performs many other actions, such as defense evasion by disabling EDR, discovery with kerberoasting attacks, and more. The end goal of this campaign is to install Interlock ransomware on victims' devices.[i]
More like Power-Down Pages	Misconfigured access controls in Power Pages, Microsoft's low-code website building alternative platform, have led to the exposure of millions of individuals' data to the public eye. Power Pages was supposed to be a tool to make life easier for those who do not have the knowledge to develop and design their own websites. Instead of implementing a least access principle by default to their product, Microsoft left those decisions up to the users. Security features that should be on by default like data masking, global permissions granted to all users, and more, have been disabled by users countless times. While Microsoft prompts its Power Pages users to make sure certain preferred security measures are taken, at the end of the day, the end user ultimately has the responsibility to make their website as secure as possible.[ii]
This is the Future of Tech?	X (formerly Twitter) user @g0njxa posted about threat actors pretending to provide an AI image and video generator service. Being mainly distributed on X, the threat actors use AI images and video examples to get the victim to go to their website to download the software. When downloaded, file analysis determined the payload to be Lumma Stealer. AMOS Stealer has also been seen in use for these attacks. The attacker has the likely goal of monetary gain, due to the theft of credentials and cryptocurrency wallets. The threat actor behind this campaign is currently unknown.[iii]
Finance Frenzy Flattens Finastra	A recent breach suffered by the financial technology firm Finastra has cost the company and its clients 400 gigabytes of data. The stolen data was then offered for sale on the cybercriminal forum BreachForums. This cyberattack can be considered significant because Finastra provides software and services to 45 of the world's top 50 banks and reported $1.9 billion in revenue last year. This event happened on November 7, with initial access seeming to come from Finastra's internally hosted file transfer platform. While few technical details on the attack were given, no malware was installed and no data was altered, making this clearly an act of financial gain and likely the result of credential reuse or misconfigured/improperly secured assets. Finastra is no longer affected by this attack, but did confirm that the 400 gigabytes of data was indeed stolen.[iv]
North Koreans for Hire	SentinelLabs has noticed a trend from North Korea of DPRK actors impersonating U.S.-based software and technology consulting businesses by copying the websites of legitimate organizations, seeking to use these for financial objectives due to sanctions currently imposed on North Korea. This is done by individuals or front companies who genuinely perform work to bring money back to North Korea. All copied decoy websites appear to be legitimate and stolen from real businesses. SentinelLabs has seen four of these fake companies in the wild, and they have all been taken offline by the U.S. government.[v]
Crossing the GLASSBRIDGE	The Google Threat Intelligence Group has been monitoring the activity of "GLASSBRIDGE," a group of four separate PR firms that bulk-creates and operates hundreds of malicious domains that mask themselves as legitimate news sites but instead publish propaganda that aligns with the interests of China. PR firms are used to establish plausible deniability, pinning the crimes on the firms. The current countries seen targeted by GLASSBRIDGE include Australia, Austria, Czechia, Egypt, France, Germany,

	Hungary, Kenya, India, Indonesia, Japan, Luxemburg, Macao, Malaysia, New Zealand, Nigeria, Poland, Portugal, Qatar, Russia, Saudi Arabia, Singapore, South Korea, Spain, Switzerland, Taiwan, Thailand, Turkey, the United States, and Vietnam. The firms also attempt to mix unrelated news into the bogus websites' newsfeeds, fooling the readers. The four firms in question are Shanghai Haixun Technology, Shenzhen Haimai Yunxiang Media (has two), and Shenzhen Bowen Media.[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
This is No Small Backdoor	The United Kingdom's National Cyber Security Centre recently published a report regarding a new backdoor designated as "Pygmy Goat."	Pygmy Goat is a Linux-based backdoor developed by an unknown threat actor. To establish C2 communication, the malware can either utilize ICMP port knocking or abuse the SSH daemon by exploiting LD_PRELOAD to hook the SSH daemon's accept function. It does so by either employing the accept function to generate a raw ICMP socket to listen for ICMP packets to elicit a callback or uses the hooked accept function to search for a sequence of magic bytes in SSH connections. Pygmy Goat's functionality includes reporting the current date and time, system information, creating System and CLI shells, using crontab to create new scheduled tasks, capturing packets, and creating reverse SOCKS5 proxies.[vii]
The Truth about ApoloStealer	Check Point Research has been following APT36, also known as Transparent Tribe, and has discovered the group has developed a new information stealer designated by CPR as "ApoloStealer."	After creating a SQLite database file, ApoloStealer collects and stores system information such as filenames, file paths, flags, types, and modified dates. Next, the malware collects all files on the victim's desktop that are not blacklisted by the stealer. Once file storage is complete, ApoloStealer sends the data to APT36's C2 server. The malware then repeats this process for other directories, such as Downloads, OneDrive, and any fixed drives other than the C drive. ApoloStealer has been attributed to APT36 partially due to ApoloStealer using techniques like other Transparent Tribe malware. One such example is that the local time zone of the malware is set to IST. Another is that the working directory is the same as SlackAPI.dll, an ElizaRAT variant. ApoloStealer also uses a similar network infrastructure and other TTPs that match APT36.[viii]
DocuGängers	Wallarm security researchers noticed a new trend regarding a surge of well-done DocuSign phishes.	This noticeable increase in quality comes from attackers leveraging DocuSign's APIs to send fake invoices from genuine DocuSign accounts and utilizing real DocuSign templates used by legitimate companies. This is done by paying for a DocuSign plan to abuse their API service for automatically crafting and mass sending phishing emails. Being properly integrated into the DocuSign communication channels themselves and containing no malicious links or attachments, this method of generating phishing emails could be problematic for detection. The goal of these operations is to get a victim to sign a fake invoice that allows the attacker to authorize payment from the victim to the attacker's bank accounts.[ix]
Infostealer Malware Proves to Be Quite the Sly Fox	Kaspersky has found a new trojan which they have dubbed "SteelFox."	Initial infection starts with presenting a loader as a piece of cracked software such as Foxit PDF Editor, JetBrains, and AutoCAD. The loader gives administrator access to be used by later malware by allowing it to install in the Program Files directory. Next, the SteelFox dropper is unpacked and decrypted from the loader, which contains another loader, this time for SteelFox, which adds itself to the victim's startup programs. The SteelFox loader then goes through multiple verification checks and injects itself into the AppInfo service for persistence. A final loader is then delivered, which carries the SteelFox trojan. It has been observed viewing many different forms of data, including browser, software, system, network, SIM, drive, environment, time, user, RDP, Desktop, and

		process data.[x]
Fabricated Fabric Fakes	The Socket Research Team has observed a malicious Python package called "fabrice" attempting to impersonate the known fabric SSH library.	The malware has been seen targeting both Linux and Windows OSs and performs different operations for both. For Linux, attackers abuse the linuxThread() function to download, decode, and execute scripts sent from the attacker. For Windows, the winThread() function is used, which contains two variables, vv and zz, that decode to be two Python scripts that work together to further infection. The vv script functions as a launcher that allows for command execution and further payload installation. Meanwhile, the zz script can download further payloads, establish persistence with scheduled tasks, and delete artifacts. The attacker's primary goal was AWS credential theft.[xi]
The Building Blocks of Ymir Ransomware	Kaspersky has uncovered a novel ransomware strain named by the company as "Ymir."	Some of the notable features of Ymir ransomware mentioned by Kaspersky include the presence of functions like malloc, memmove, and memcmp making API calls, indicating that it can allocate memory to inject code. The malware uses another function to gather system information by using more API calls. CryptoPP, a C++ cryptographic library, was also used to borrow more functions for Ymir. The ChaCha20 algorithm is also used for file encryption. This ransomware has been seen recently targeting Columbian victims, with the initial infection coming from the use of RustyStealer.[xii]
Venerable Remcos RAT Gets a New Coat of Paint	Fortinet's FortiGuard Labs have been seen putting in the work regarding their discovery of a new variant of Remcos RAT.	The most important thing to take away from this novel Remcos RAT variant is its ability to deploy itself in running processes' memory, meaning that the malware is now fileless. It can also run commands against benign software to gather information, such as manipulating File Manager to create, modify, or delete files, run Process Manager to see all running processes, and establish a remote shell, run scripts remotely, turn on keylogging functions, and more. In more general terms, the new Remcos RAT variant contains improved features for persistence, evasion, and remote access control.[xiii]
Watch Out for the Data Goblin!	The Solar 4RAYS team unexpectedly discovered a new RAT which the team has designated as "GoblinRAT."	Written in Golong, GoblinRAT has the main objective of granting malware defense evasion. However, it has many other functionalities as well, such as opening remote shells, command execution, file system enumeration, creating, modifying or deleting files, SOCKS5 proxy capabilities, and Yamux features. The RAT is described as working in four stages: configuration decryption, defense evasion, connection to the attacker's C2 server, and command execution (in that order). Some of the previously mentioned defense evasion tactics include renaming processes, deleting backups, and more. Commands possible include taking screenshots, opening ports, archiving files into ZIP format to exfiltration, and more.[xiv]
Another Day, Another Not-So-Novel Infostealer	Cisco Talos has shown the public its findings on a new information stealer called "PXA Stealer."	PXA Stealer is delivered through a ZIP file attached to a phishing email, which leads to a loader written in Rust if opened that runs multiple scripts to execute PXA Stealer. The stealer can collect data on login information, browser cookies, autofill information, credit card details, Facebook ads account data, cryptocurrency wallet data, Discord token details, and MinSoft application data. Cisco Talos believes that the campaign currently orchestrating the use of PXA Stealer is CoralRaider, because the attacker sells collected data in the same Telegram channel as CoralRaider and is in Vietnam, based on collected domain registration data.[xv]

Yer a Wezard, Rat!	Thanks to a combined effort from the FBI, the U.S. Department of Treasury, the Israeli National Cybersecurity Directorate (INCD), and Check Point Research, we have information on the newest variants of WezRat.	This newest WezRat campaign starts by impersonating the INCD to send phishing emails to various Israeli organizations. The phishing emails contain a link to download a fake Google Chrome install MSI file. This not only legitimately installs Chrome but also installs WezRat. Once installed, the RAT communicates back and forth from the attacker's C2 infrastructure, sending data and receiving commands. The newer variants feature aspects such as defense evasion via opaque predicates and control flow flattening. WezRat also no longer contains hardcoded C2 server addresses within itself and now requires a password to run. Other differences include WezRat's new screenshot and keylogger abilities.[xvi]
RustyAttr Comes with New Tricks	Group-IB researchers have identified the use of a new technique to evade detection, along with a new trojan used by the APT group Lazarus to target macOS users.	To start, the new technique employed by Lazarus uses a file's extended attributes to hide malicious code within the file's metadata and out of the sight of detections. In fact, because of this, the files are currently fully undetected on VirusTotal and likely other forms of detection as well. The new trojan associated with this activity is known as "RustyAttr." The end goal of this campaign is not currently known as no further stages of the attack were able to be captured.[xvii]
Melofee Does Not Chill	XLab has recently announced the appearance of a new variant of the Melofee backdoor.	The malware now has two modes it can function in, infection and management mode. Infection mode allows the user to establish persistence with crontab, disguise process names, files, processes, and directories, along with C2 capabilities. Management mode controls Melofee's stealth functionalities, determining whether to hide or act. Some new stealth capabilities include using hidden kernel drivers and hiding HTTPS traffic. The malware also now uses RC4 encryption and can help issue commands from the attacker's C2 through ioctl calls. Interestingly, this variant is used to target systems running Red Hat Enterprise Linux (RHEL) 7.9 with a kernel version of 3.10.0.[xviii]
Issues in the Inbox	SlashNext publicized a new malware find which is advertised on Telegram as "Golssue" by a member of the threat group "Gitloker Team."	Golssue is a tool that is used to extract email addresses from publicly available GitHub profiles and send mass quantities of phishing emails directly to the victims' inboxes. These phishing emails are made to look like GitHub notification emails, which only further convinces the victim the email is legitimate. The malware's ability to send thousands of these phishes at once is also quite alarming. Due to Golssue's connections to the Gitloker Team, SlashNext suggests it is likely being used in their current campaign.[xix]
New Malware Takes Flight	Jamf Threat Labs has shed light on a wave of new malware being built using the Flutter framework.	Flutter is a framework developed by Google to allow for cross-platform app design. Thus, by using Flutter, a developer can have their software be consistent across Windows, MacOS and iOS, and Android mobile devices. Malware made using Flutter that Jamf Threat Labs has identified recently are all .app files and were developed in different languages such as Go and Python. The malware is made to appear benign, opening what appears to be the Minesweeper game or a Notepad file. Commonly, however, these files reach out to known DPRK malware domains. Unfortunately, at the time of analysis, the threat actor-controlled domains were taken offline, so the second stage of this attack is unknown. The group behind the attack is also currently unknown but is suspected to have ties to North Korea.[xx]
The Newest Bane in Malware	ESET researchers have recognized two novel Linux backdoors used by the Gelsemium APT	These backdoors, named "WolfsBane" and "FireWood," are believed to be derived from previous Gelsemium malware, such as Gelsevirine for WolfsBane and FireWood having connections to Project Wood. It is believed that Gelsemium first

	group.	accesses victims through using webshells targeting vulnerable web applications. The victims receive an archive file that contains the malware. When executed, a WolfsBane dropper activates, dropping the WolfsBane launcher and WolfsBane itself. After installation, WolfsBane can begin to communicate with the threat actor's C2. FireWood is also included in the initial archive file and has its own unique functionalities such as establishing persistent access, loading and unloading kernel modules, and other backdoor-related activity.[xxi]
These Spies Bring the Wrong Vibe	Insikt Group has shown proof regarding the existence of two new custom malware tools used by APT28.	These tools, "HATVIBE" and "CHERRYSPY," have been used by APT28 to target government entities, human rights groups, and educational institutions in Central Asia, East Asia, and Europe. The malware works together, with HATVIBE being an HTML loader used to deploy CHERRYSPY, a Python-based backdoor. It is believed that HATVIBE is delivered though either malicious email attachments or exploited web-facing vulnerabilities and helps achieve persistence through scheduled tasks. CHERRYSPY is then used for secure data exfiltration, using RSA and AES for encryption, to send stolen data and receive commands from APT28's C2 servers.[xxii]
Hex On, Hex Off	In August, CYFIRMA discovered a Telegram channel advertising a new information stealer sold as "Hexon Stealer."	Hexon Stealer is a Discord-based information stealer with many data stealing options, including Discord tokens, 2FA backup codes, browser cookies, autofill data, saved passwords, credit card details, and cryptocurrency wallet information. To function, Hexon uses Electron for its desktop application interface and is packaged using NSIS to distribute its malicious payload. The malware's main goals are Discord process injection, accessing gaming-related accounts, and stealing cryptocurrency. Upon successful installation, Hexon's remote capabilities include screenshotting, fake prompt messages, establishing direct messaging with the victim, gaining full control of the affected device, and more.[xxiii]
JinxLoader Meets its New Fate	The BlackBerry Research and Intelligence Team noticed a change recently in the loader malware JinxLoader, changing branding from JinxLoader to "Astolfo Loader."	JinxLoader was sold to a new threat actor who renamed the malware and modified it to run on C++ instead of Go. This change was made to achieve a smaller size and improved performance compared to JinxLoader, with Astolfo Loader decreasing size from 5.5 MB to 120 KB for the x64 version and 110 KB for the x86 version. New features of Astolfo include running remote commands and anti-analysis measures. It is also important to note that the original JinxLoader is still active.[xxiv]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Breaking the Meta with Venture Wolf	BI.ZONE Threat Intelligence has alerted the public to a potential new threat actor which BI.ZONE has designated as "Venture Wolf." So far, the group has been seen delivering malicious archive files containing various loaders used to download Venture Wolf's intended final payload, the information stealer MetaStealer. These loaders will either create a .NET file to inject the malicious payload into or instilling itself into the RegAsm.exe process to avoid detection. The loaders use multiple WinAPI functions to inject code, with their names being CreateProcessW, VirtualAllocEx, WriteProcessMemory, Wow64SetThreadContext, SetThreadContext, and ResumeThread. The process starts with CreateProcessW generating a process in either the dummy .NET file or RegAsm.exe. Next, VirtualAllocEx is used to allocate memory to the generated process. Third, WriteProcessMemory writes the MetaStealer payload into an allocated section of memory. Following this, Wow64SetThreadContext and SetThreadContext change the thread context to establish the entry point for the MetaStealer payload. Finally, ResumeThread transfers control over to MetaStealer, starting the information stealing process.[xxv]
APT32 Transforms Their Attack Vector	The QiAnXin Threat Intelligence Center has seen new activity from APT32, also known as OceanLotus, involving its new use of the MSI transforms technique, which allows for the customization of existing MSI-based software before installation. The group's current attack chain starts with a spear phishing email containing an IMG file that holds a malicious LNK file. The LNK then runs the command "msiexec\.exe /qn /i WindowsPCHealthCheckSetup\.msi TRANSFORMS=msGFG\.mst," performing the MSI transforms technique and then sideloads a malicious DLL file containing the RUST trojan to install on the victim's devices, which is APT32's end goal with the campaign.[xxvi]
Don't Fall for This Phishing Trap!	The Securonix Threat Research team has been following a campaign they have designated as "CRON#TRAP" that has a unique attack methodology. Although unable to confirm the initial stages of the attack, Securonix believes the attack begins with a phishing email containing a ZIP file. Inside the archive are both a shortcut file masquerading as a survey and a data folder holding a QEMU installation directory. The shortcut runs a PowerShell command that runs start.bat, a file that dismisses suspicions with a fake error screen and runs the QEMU VM. This VM holds a backdoor within itself that allows the adversaries to connect to their C2 environment, allowing for stealthy operation. PivotBox is also in the VM and has many capabilities like reconnaissance, persistence, privilege escalation, and more. Finally, a Chisel client was also found on the VM, which has been modified to function similarly to a backdoor, enabling another avenue of C2 communication.[xxvii]
The CopyRh(ight)adamantys Campaign Comes Packed With OCR	Check Point Research (CPR) has found a campaign, which they have named "CopyRh(ight)adamantys," pushing a new variant of the known Rhadamanthys information stealer. The malware is sent through spear phishing emails that contain a malicious link to the attacker's Dropbox or Discord to download the archive file containing the stealer. This archive file contains a packed Rhadamanthys copy, along with an executable used to unpack it and a decoy file to avoid suspicion. The main addition to Rhadamanthys that CPR has mentioned is its new OCR component, allowing for the malware to search for keywords on a victim's device involving cryptocurrency. This shows a financial gain incentive rather than that of espionage. Targets of the campaign further this claim, having attempted to steal data from countries all around the globe.[xxviii]
A Stolen Wage Can Lead to Rage	Zscaler ThreatLabz has made connections between Contagious Interview and WageMole, two active North Korean cyber campaigns that attempt to either steal cryptocurrency or get past imposed political sanctions by disguising as a remote worker to be legitimately paid by employers. While WageMole mainly uses social engineering to coerce their targets to hire them, Contagious Interview employs a more malicious

	approach. Victims are often infected with BeaverTail, which is done by the threat actors either uploading malicious NPM packages containing BeaverTail to GitHub or injecting BeaverTail into legitimate NPM projects. The malware is designed for data theft and to load further stages of malware, such as a Python-based backdoor known as InvisibleFerret. While BeaverTail targets cryptocurrency wallets and credit card information stored in victims' web browsers, InvisibleFerret is used for sending system information and exfiltrating data from victims to the threat actor. With the acquired data, they can either steal cryptocurrency directly from the victim or impersonate them and carry out an attack similar to WageMole.[xxix]
VEILDrive UnVEILed	Hunters' Team AXON has identified a new campaign that the company has dubbed "VEILDrive." The VEILDrive campaign works through a previous victim's Microsoft Teams account that is compromised in some way, facilitating social engineering against further victims who believe the account is legitimate. Next, the attackers use Microsoft Teams to message select non-technical employees at the next victim's organization. The compromised account then impersonates an IT team member for the company and requests access to devices through the Quick Assist RDP tool. Once the actor gains access to the victim's device with Quick Assist, a ZIP file is downloaded which includes more RMM tools. Scheduled tasks are also made to establish persistence, opening the attacker's RMM tools whenever startup occurs. Next, the main custom Java-based malware is downloaded to the victim's device and executed. When executed, Team AXON noticed its multiple DNS connections to external domains, along with attempts to gather system information. They then finally add the custom Java malware as a registry entry to allow for automatic startup upon login.[xxx]
New Threat Group Has Yet to Have Their Kairos Moment	Cyjax had a great find recently with the discovery of a newly formed extortion group calling themselves "Kairos." Kairos does not associate themselves with ransomware, instead aiming solely for data theft. The group's main target appears to be medium-sized businesses within United States, specifically the healthcare sector. The group's data-leak site has many rules for victims to follow, such as making payment through Bitcoin and having only seven days to submit payment. Unfortunately, due to the group being so new, their attack methodology is unknown at this time.[xxxi]
APT41's LightSpy Campaign Ramps Up with New 'DeepData' Malware	BlackBerry has kept tabs on the LightSpy malware campaign, likely to be associated with the China-backed threat group APT41. In their recent discoveries, they have found APT41 using "DeepData," a new, modular, Windows-based malware framework, along with 12 plugins that can be used by DeepData, and more. With DeepData comes a plethora of actions that can be taken, ranging from reconnaissance to data theft. This is made possible through the use of the plugins to give DeepData further capabilities, such as the Appdata plugin, which collects data from IM clients or the SystemInfo plugin which collects information on a victim's device. The main goal of DeepData appears to be data theft and since they are state affiliated with China, it can be assumed that this malware will likely be used for espionage purposes.[xxxii]
Earth Estries Vampiric Relationship with Data	Trend Micro recently cleared the air regarding Earth Estries and the two most common attack chains used in their campaigns. The first attack chain targets vulnerable or misconfigured QConvergeConsole installations for initial access, then installs a remote agent to perform network discovery. PSExec is then used to laterally install various backdoors and tools by using CAB files containing the backdoors or tools. One of the backdoors downloaded is Cobalt Strike, which is used for its backdoor capabilities and to deploy the second-stage backdoor, Crowdoor. The information stealers TrillClient, Crowdoor, and Cobalt Strike are then used to steal data and exfiltrate it back to the attackers. For the second chain, ChinaCopper is used for initial access into Microsoft Exchange servers. PortScan is used for network discovery and three tools are then used for lateral movement and persistence, which are Cobalt Strike, Zingdoor, and Snappybee. Zingdoor is also used for lateral movement and a hack tool called NinjaCopy is used for credential access. Data is then collected through RAR archive and cURL is used to exfiltrate the stolen data.[xxxiii]
LIMINAL PANDA Makes Their Debut	Crowdstrike has been tracking a previously undisclosed threat group since 2020 that the organization has dubbed "LIMINAL PANDA." Due to its connections to China, it is believed that LIMINAL PANDA's main motivation is espionage. So far, the group is known for their part in LightBasin campaigns. They have also been seen with many in-house developed tools and malware such as "PingPong," "CordScan,"

	"SIGTRANslator," and tools used in the LightBasin campaigns such as StealthProxy, BridgeTroll, and cdr_xf. The current main targets for LIMINAL PANDA are telecommunications providers in southern Asia and Africa.[xxxiv]
IRGC Actors Continue Muddying the Waters	Sophos MDR has spotted a new MuddyWater campaign that uses spear phishing to trick their targets into downloading a legitimate RMM tool to dump credentials. Each phish has a ZIP attachment containing the RMM tool Atera, using a trial account to use the service freely and temporarily. After the Atera Agent is installed, MuddyWater used Atera to execute a PowerShell script with the goal of dumping victim credentials and creating a backup file of the SYSTEM registry hive. Once all the desired data has been copied, the stolen information is then sent back to the attackers through an SSH tunnel.[xxxv]
Ursnif Remains an Annoying Nuisance	A new campaign has been exposed by Cyble's Research and Intelligence Labs pushing the Ursnif trojan. The campaign begins with a phishing email containing a ZIP file that holds a malicious LNK file disguised as a PDF. The LNK holds a command that, upon execution, runs CertUtil to decode and activate a malicious HTA file embedded within the file. This HTA is run by mshta.exe and drops a PDF as a decoy, along with a DLL loader that contains Ursnif. This DLL is where communication between the attacker and the infected machine begins. The threat actor behind this campaign is currently unknown.[xxxvi]

Dark Web Markets

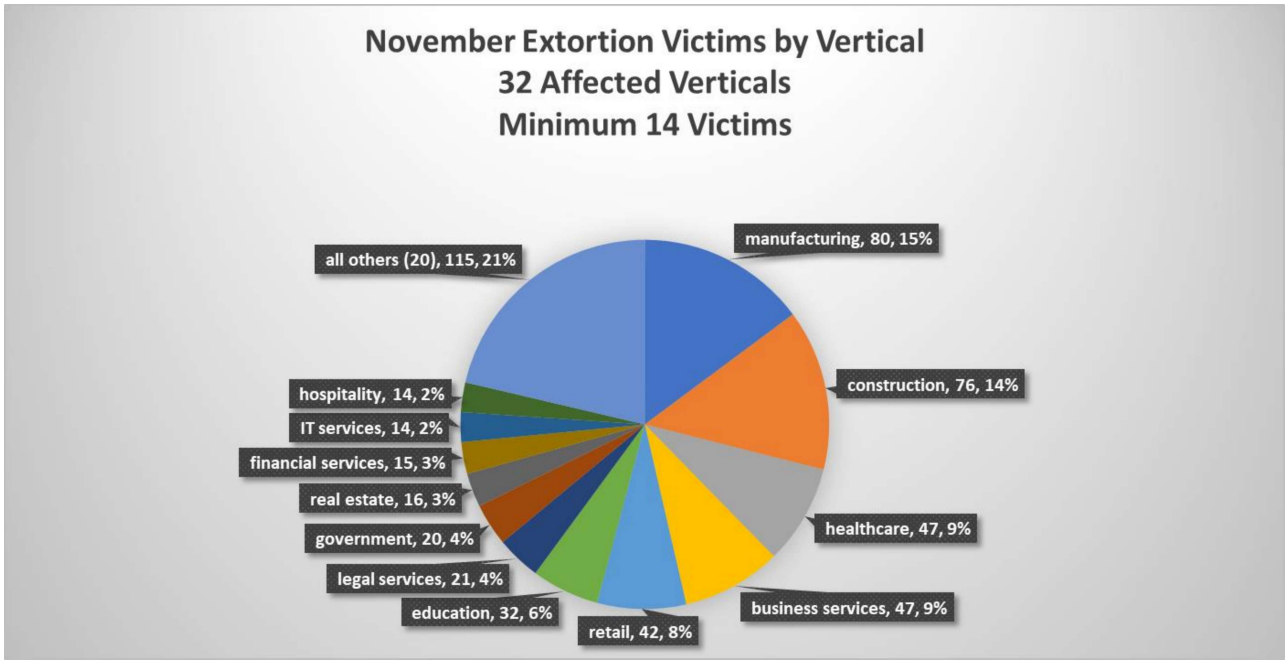
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

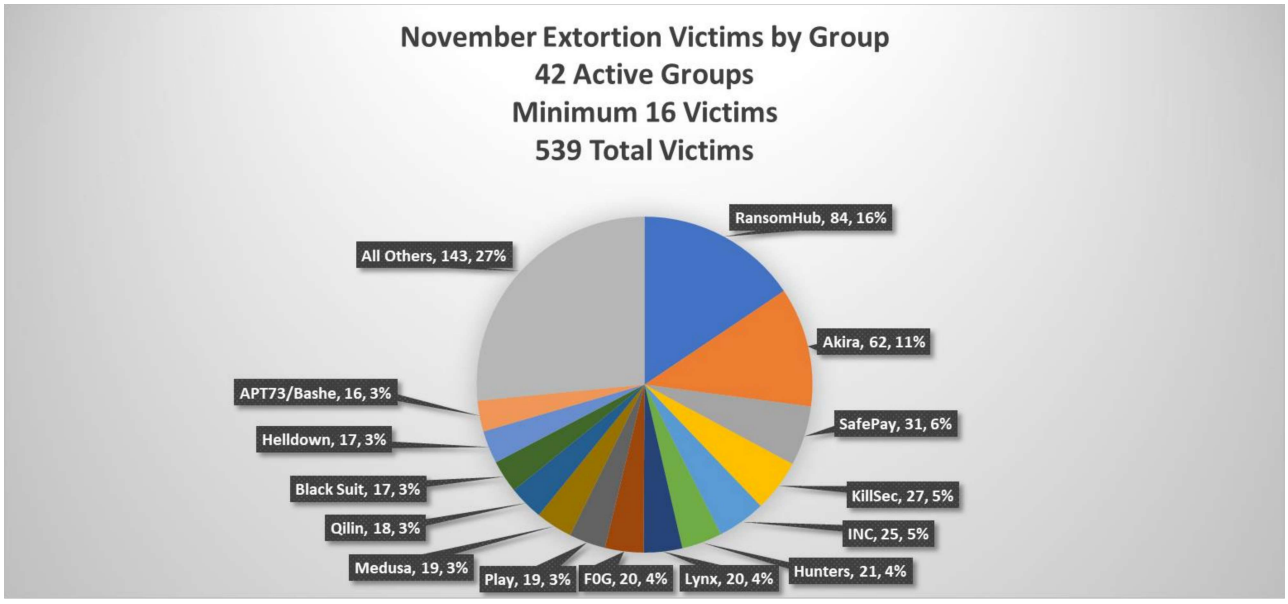
Activity	Note
Actor Developments	The actor who exploited vulnerabilities in Snowflake to compromise dozens of companies was arrested in Canada. Connor Riley Moucka, AKA Judische AKA Waifu, was arrested in Ontario, Canada and charged with multiple counts of stealing data and extorting from dozens of companies. Moucka and two accomplices advertised and attempted to sell the data on Breach Forums and the Russian language crime forums XSS and Exploit.
Data Sale	An actor posted a Google Drive link to what he claims was 8 GB of data stolen from a Fairfax, Virginia-based access management company. The actor claimed that the file contained more than 10,000 files, including .p7s and .p12 cryptographic key files. The actor further claimed that numerous companies were impacted by the breach. The claims could not be independently verified because Google removed the file within three hours of posting.
Data Sale	An actor was observed selling what he claimed was a U.S. Military database containing information pertaining to more than 385,000 service people and contractors, including name, email, phone, service, component, primary job, unit information, and location. Judging from the sample posted, some of the service members are in sensitive positions.
Access Sale	An access seller was observed selling Citrix access to an enterprise in Germany in the automobile parts vertical with USD 2.4 billion in revenue for USD 8,000. A prolific ransomware actor expressed interest in buying the access.
Tool Sale	A well-known crime forum actor announced the return of the DarkGate loader. The price is USD 8,000 for a one-month license or USD 18,000 for a three-month license. They posted multiple videos purporting to demonstrate runtime bypass using AutoIT and VBS. They further posted a screenshot of the control panel showing DarkGate v7.0.7. Later the actor was banned from the crime forum for refusing to use the forum escrow to secure deals. This does not mean the malware is off the market, it just means the actor can't advertise in one of the most active crime forums.
Access Sale	A senior actor on a popular crime forum and probable member of the new Hellcat extortion team was selling "access to server hosting firewall" to several dozen victims, including: - The largest European film studio with USD 50 million in revenue for USD 500 - A French energy distributor with USD 7 billion or EUR 7 billion in revenue for USD 1,000 - A U.S.-based university with USD 5.6 billion in revenue for USD 1,500 - An unnamed industrial IoT and computing company with USD 2 billion in revenue for USD 1,000 - An unnamed consulting engineering company with USD 30 million in revenue for USD 500 - An unnamed U.S. medical center with USD 30 million in revenue for USD 1,000 - An unnamed U.S. government healthcare organization with USD 4 billion in revenue for USD 1,500 Cybersecurity practitioners on X speculated (without evidence) that the actor may be exploiting Fortinet CVE-2024-23113 or the new Palo Alto PanOS 0day.
Data Sale	An actor on a popular Russian-language crime forum claimed that they and the well-known owner of another popular crime forum compromised a major American automobile manufacturer, exposing the names and data of 44,000 customers.
Access Sale	An actor was observed selling shell access to a U.K.-based accounting and business services company with USD 50 billion in revenue for USD 25,000.
Access Sale	An actor was observed selling Cisco access to an unidentified U.S.-based "space manufacturing" company with USD 500 million in revenue and 500 employees for USD 5,000.
Data Sale	An actor claimed to have access to a major real estate broker and exfiltrated 21 TB of data. They posted a 2 GB sample of data to prove access. They were demanding USD 75,000 for the data and access to the network.

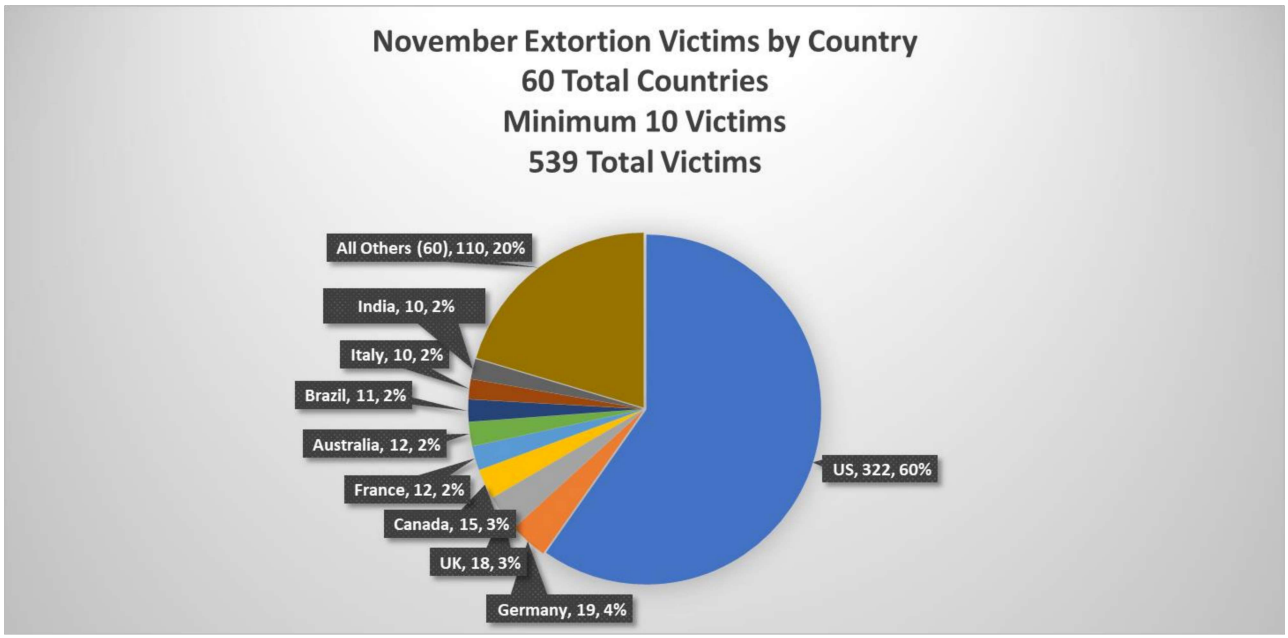
Actor Developments	In their first post on a popular crime forum, an actor announced that they are looking to buy a private working exploit for CVE-2024-38077 Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability. Their announced budget was USD 5,000-9,000. The purpose for this exploit is unknown.
Access Sale	An actor associated with the Hellcat extortion team has placed at least 43 victims up for sale for prices ranging from USD 300-1,000. There are few details for each victim; only two victims had a revenue range indicated. All privileges are "access to server hosting firewall" with no further information. The victims include: - A U.S. paper company with USD 17 billion in revenue - A U.S. computer science university - A major US Catholic university - A U.S. public health agency - A U.S. IT consulting company - A major California university - A Korean semiconductor company - A Korean helicopter sales company - A US cybersecurity company with USD 100 million in revenue - A major US university - A U.S. "major IoT leader" with USD 2 billion in revenue - A U.S. private equity firm - A U.S. multi-state water management agency - A U.S. Department of Defense cybersecurity contractor - A Florida healthcare enterprise - A UK electric grid management company - The U.S. Department of Defense Joint Task Force tactical communications application - A U.S. hazardous materials emergency response entity - A U.S. international airport - A Pennsylvania college - A U.S. local internet provider - A U.S. telecom provider - A U.S. semiconductor manufacturer - A U.S. major infrastructure provider

By The Numbers

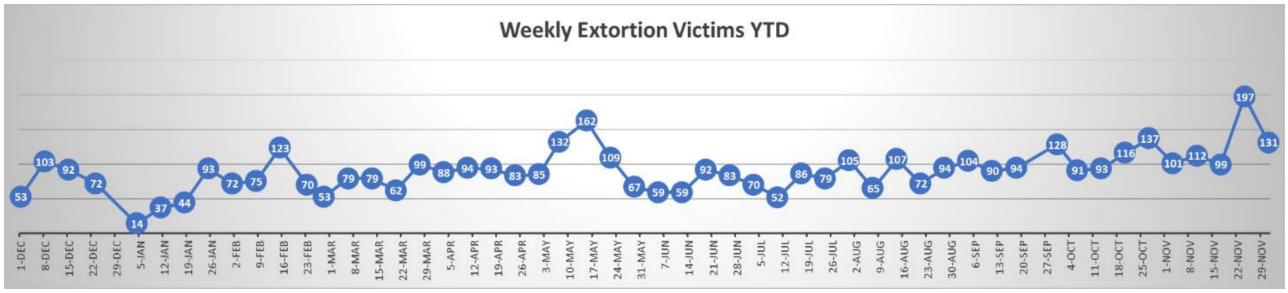
Summarizing incidents in graphical format






November Extortion Victims by Country
60 Total Countries
Minimum 10 Victims
539 Total Victims
All Others (60), 110, 20%
India, 10, 2%
Italy, 10, 2%
Brazil, 11, 2%
Australia, 12, 2%
France, 12, 2%
Canada, 15, 3%
UK, 18, 3%
Germany, 19, 4%
US, 322, 60%


Monthly Victim Count
260
318
319
443
470
293
392
338
416
538
539
JANUARY
FEBRUARY
MARCH
APRIL
MAY
JUNE
JULY
AUGUST
SEPTEMBER
OCTOBER
NOVEMBER


Weekly Extortion Victims YTD
53
103
92
72
14
37
44
93
72
75
123
70
53
79
79
62
99
88
94
93
83
85
132
162
109
67
59
59
92
83
70
52
86
79
105
65
107
72
94
104
90
94
128
91
93
116
137
101
112
99
197
131
1-DEC
8-DEC
15-DEC
22-DEC
29-DEC
5-JAN
12-JAN
19-JAN
26-JAN
2-FEB
9-FEB
16-FEB
23-FEB
1-MAR
8-MAR
15-MAR
22-MAR
29-MAR
5-APR
12-APR
19-APR
26-APR
3-MAY
10-MAY
17-MAY
24-MAY
31-MAY
7-JUN
14-JUN
21-JUN
28-JUN
5-JUL
12-JUL
19-JUL
26-JUL
2-AUG
9-AUG
16-AUG
23-AUG
30-AUG
6-SEP
13-SEP
20-SEP
27-SEP
4-OCT
11-OCT
18-OCT
25-OCT
1-NOV
8-NOV
15-NOV
22-NOV
29-NOV

New Detection Content

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

- **Attempt To Delete Services**
  - Platform: Splunk
  - The following analytic identifies Windows Service Control, `sc.exe,` attempting to delete a service. This is typically identified in parallel with other instances of service enumeration of attempts to stop a service and then delete it. Adversaries utilize this technique to terminate security services or other related services to continue their objective and evade detections.

- **Delete A Net User**
  - Platform: Splunk
  - This analytic will detect a suspicious net.exe/net1.exe command-line to delete a user on a system. This technique may be used by an administrator for legitimate purposes; however, this behavior has been used in the wild to impair users or delete adversaries' tracks created during its lateral movement in additional systems. During triage, review parallel processes for additional behavior. Identify any other user accounts created before or after.

- **Resize Shadow Storage Volume**
  - Platform: Splunk
  - The following analytic identifies the resizing of shadow storage using vssadmin.exe to avoid the shadow volumes being made again. This technique is typically used by adversaries during a ransomware event and a precursor to deleting the shadow storage.

- **Potential Pass the Token or Hash Observed by an Event Collecting Device**
  - Platform: Splunk
  - This detection identifies potential Pass the Token or Pass the Hash credential stealing. We detect the main side effect of these attacks, which is a transition from the dominant Kerberos logins to rare NTLM logins for a given user, as reported by an event-collecting device (i.e., a specific domain controller or an endpoint destination).

- **Potential Pass the Token or Hash Observed at the Destination Device**
  - Platform: Splunk
  - This detection identifies potential Pass the Token or Pass the Hash credential stealing. We detect the main side effect of these attacks, which is a transition from the dominant Kerberos logins to rare NTLM logins for a given user, as reported by a destination device.

- **Wevtutil Usage to Disable Logs**
  - Platform: Splunk
  - This search is to detect execution of wevtutil.exe to disable logs. This technique was seen in several ransomware incidents where the attackers utilized webtutil.exe to disable the event logs to evade alerts and detections in a compromised host.

[i] https://blog.talosintelligence.com/emerging-interlock-ransomware/
[ii] https://www.darkreading.com/cybersecurity-operations/microsoft-power-pages-millions-private-records
[iii] https://www.bleepingcomputer.com/news/security/fake-ai-video-generators-infect-windows-macos-with-infostealers/
[iv] https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
[v] https://www.sentinelone.com/labs/dprk-it-workers-a-network-of-active-front-companies-and-their-links-to-china/
[vi] https://cloud.google.com/blog/topics/threat-intelligence/glassbridge-pro-prc-influence-operations
[vii] https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/pygmy-goat/ncsc-mar-pygmy-goat.pdf
[viii] https://research.checkpoint.com/2024/the-evolution-of-transparent-tribes-new-malware/
[ix] https://lab.wallarm.com/attackers-abuse-docusign-api-to-send-authentic-looking-invoices-at-scale/
[x] https://securelist.com/steelfox-trojan-drops-stealer-and-miner/114414/
[xi] https://socket.dev/blog/malicious-python-package-typosquats-fabric-ssh-library
[xii] https://securelist.com/new-ymir-ransomware-found-in-colombia/114493/
[xiii] https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims
[xiv] https://rt-solar.ru/solar-4rays/blog/4861/
[xv] https://blog.talosintelligence.com/new-pxa-stealer/
[xvi] https://research.checkpoint.com/2024/wezrat-malware-deep-dive/
[xvii] https://www.group-ib.com/blog/stealthy-attributes-of-apt-lazarus/
[xviii] https://blog.xlab.qianxin.com/analysis_of_new_melofee_variant_en/#background
[xix] https://slashnext.com/blog/goissue-github-phishing-attacks/
[xx] https://cyberscoop.com/wp-content/uploads/sites/3/2024/11/FINAL-Jamf-macOS-Flutter-DPRK-Research.pdf
[xxi] https://www.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-gelsevirine/
[xxii] https://www.recordedfuture.com/research/russia-aligned-tag-110-targets-asia-and-europe
[xxiii] https://www.cyfirma.com/research/hexon-stealer-the-long-journey-of-copying-hiding-and-rebranding/
[xxiv] https://blogs.blackberry.com/en/2024/11/jinxloader-evolution
[xxv] https://bi-zone.medium.com/venture-wolf-attempts-to-disrupt-russian-businesses-with-metastealer-cddb6edb07c8
[xxvi] https://ti.qianxin.com/blog/articles/new%20-trend-in-msi-file-abuse-new-oceanlotus-group-first-to-use-mst-files-to-deliver-special-trojan-en/
[xxvii] https://www.securonix.com/blog/crontrap-emulated-linux-environments-as-the-latest-tactic-in-malware-staging/
[xxviii] https://research.checkpoint.com/2024/massive-phishing-campaign-deploys-latest-rhadamanthys-version/
[xxix] https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west
[xxx] https://www.hunters.security/en/blog/veildrive-microsoft-services-malware-c2
[xxxi] https://www.cyjax.com/resources/blog/an-elephant-in-kairos-data-leak-site-emerges-for-new-extortion-group/
[xxxii] https://blogs.blackberry.com/en/2024/11/lightspy-apt41-deploys-advanced-deepdata-framework-in-targeted-southern-asia-espionage-campaign
[xxxiii] https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html
[xxxiv] https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/
[xxxv] https://news.sophos.com/en-us/2024/11/20/sophos-mdr-blocks-and-tracks-activity-from-probable-iranian-state-actor-muddywater/
[xxxvi] https://cyble.com/blog/ursnif-trojan-hides-with-stealthy-tactics/