Monthly Threat Intelligence Rollup

DEEP seas

10/01/24-10/31/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Royal Mail Impersonators Proving a Royal Pain	Proofpoint researchers have uncovered a new ransomware campaign delivering Prince ransomware, which claims to be an "educational tool" available for free on GitHub. In these Prince ransomware attacks, the unknown assailants posed as employees of the British postal service, Royal Mail, targeting organizations in the U.K. and the U.S. in September. The attackers' delivery method of choice was phishing; however, they also have been seen initiating communication through contact forms made public on victims' websites. The emails contained a PDF attachment that included a link to download a ZIP file hosted on Dropbox. That ZIP file held a LNK file containing JavaScript. This LNK file facilitated the creation of multiple PowerShell scripts which abuse known vulnerabilities and allow for the decryption and extraction of Prince ransomware. Interestingly, there were no decryption or data exfiltration methods available in this Prince ransomware strain once files were encrypted, showing that the attacks were not financially motivated.[i]
All Eyes on Callisto	The FBI has filed a seizure of over 41 domains belonging to the Callisto Group, a threat group part of the Russian Federal Security Service (FSB), specifically Center 18, also known as the Centre for Information Security Military Unit 64829. The FBI made the seizure because the domains are used in phishing campaigns with the goal of gaining access to their victims' devices or accounts and exfiltrating data for espionage. However, this is not the end of the story for Callisto Group. Microsoft has also shown interest in taking down Callisto Group's malicious domain infrastructure, filing for an additional 66 domains to be seized by the FBI. Similarly to the previous domains, these malicious websites were also used in phishing lures to steal data for espionage. While not taken down yet, due to the previous takedown of Callisto Group domains, the case is likely to go in Microsoft's favor.[ii] [iii]
Donot Mess with This Group	360 Advanced Threat Research Institute has made clear that APT-C-35, also known as Donot, is still going strong and is actively stealing sensitive data from government entities in South Asia, with the most common target being Pakistan. To do so, APT-C-35 will do one of the following first: either deploy a decoy file with macros embedded to execute shellcode and download the malicious DLL from the group's servers or use a template injection to load an RTF document that contains a Microsoft Office vulnerability (CVE-2017-11882) that would allow for the malicious DLL to be downloaded. While not stated in the article, it is likely that, since their attack process exploits Office vulnerabilities, the initial delivery vector will be phishing.[iv]
A Case of Stolen Identity	Trend Micro presented their findings on a surge of Golang ransomware targeting Amazon's S3 (Simple Storage Service) Transfer Acceleration feature to exfiltrate sensitive data from victims and upload said data to the attacker's S3 buckets. To expediate a ransom payment, the unknown assailants disguised the ransomware as LockBit ransomware, a much higher profile threat group. For each victim UUID acquired, a new S3 bucket is spun up on the attacker's side. Thankfully, however, from the Golang samples recovered, all AWS access key IDs and the secret access keys were hard-coded, which allows for easy detection of this ransomware strain. Because of this, these AWS access keys have been suspended by Amazon from using their services.[v]
A Silent Poisoning	Kaspersky has brought an ongoing campaign targeting Russian victims to the attention of the public. The attacks start through the SEO poisoning of Yandex search results, displaying fake webpages that claim to download software like uTorrent, Microsoft Excel, Microsoft Word, Minecraft, Discord, and more for free. They also distribute malware through comments containing links in YouTube videos the attackers publish. Once a victim takes the bait, a ZIP file that contains a MSI and TXT file is downloaded, the MSI file being the malware itself and the TXT file holding the password to begin installation.

	Next, a VisualBasic script is run, which then opens a BAT file that helps with privilege escalation. Further actions are taken after this for persistence, including allowing for the deployment of a reverse shell and replicating itself to avoid deletion. The goal of this campaign is to install “SilentCryptoMiner” onto victim devices to mine cryptocurrency.[vi]
RansomHub Targets Mexican Airspace	On October 15, Grupo Aeroportuario del Centro Norte, also none as OMA, a Mexican airport operating company, publicized that they were victims of a cyber attack and had to rely on backup systems to continue running the 13 airports they control. The attack was claimed to be done by the RansomHub group, who threatened to leak three terabytes of stolen data from OMA if a ransom was not paid. The ransom amount and contents of the stolen data are currently unknown to the public. Besides their main systems being taken offline and data stolen, there has been no other effects on the business, demonstrating that RansomHub was only able to accomplish the above malicious actions. OMA is following up this breach with a collaboration between their own IT team and external cybersecurity experts.[vii]
Leaky Plane Oil Tanks	Cybersecurity researchers in CloudSEK’s TRIAD division updated the public regarding new activity from Iran’s APT34, also known as OilRig. The group is continuing to target other Middle East countries for espionage purposes but has moved their attention to the aerospace sector. This interest seems to be caused by Iran’s curiosity of aerospace research and technology in the Middle East. The group’s likely goal is to exfiltrate sensitive intellectual property, which could disrupt the aerospace market on a global scale. APT34 has been achieving this by first gaining access through exploiting a critical privilege escalation vulnerability in the Windows Kernel of Microsoft Exchange servers, going by CVE-2024-30088. Following this, the group moved laterally through the network, establises persistence measures, and steals credentials and data.[viii]
Hacker Frees Private Customer Data	A large French ISP called Free, that boasts over 22 million subscribers, was attacked by BreachForums user “drussellx” and had customer information stolen. The attack was mainly directed toward a management tool that held subscriber data that, according to drussellx, affects all Free Mobile and Freebox customers and contains over 5.11 million International Bank Account Numbers. The bad actor has posted proof, including stolen data, screenshots, and database headers, and has said they would be willing to let customers search through what was stolen to confirm it was Free’s entire customer database. Thankfully, however, they failed to access customer passwords, bank card information, and any communications, such as emails or SMS. Furthermore, Free insists that only certain fixed subscribers were impacted and not to a large degree.[ix]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
FIN7's New Ambitious Scam	Silent Push threat analysts shared an update regarding their research into the financially motivated, Russia-based threat group, FIN7.	Their discoveries point out two malware honeypot methods FIN7 continues to actively use. The first uses multiple websites that put up a front of distributing a new "AI Deepnude generator", which is either offered by FIN7 for free or behind the guise of a "free trial." The second uses a scam that FIN7 has used previously, a "Requires Browser Extension" scheme. The idea for this form of social engineering is to appear like a legitimate site where a popup requiring the installation of a browser extension is shown, allowing the user to download malware from the site. Some of the malware seen from these various scams include NetSupport RAT, Redline Stealer and D3F@ck loader.[x]
BabyLockerKZ Gives Businesses Something to Cry About	Cisco Talos posted an advisory on a variant of MedusaLocker ransomware, named "BabyLockerKZ" by its unknown, financially motivated threat actor.	While BabyLockerKZ has been around since 2022, its coverage has been sparse due to it being almost identical to MedusaLocker besides some different keys and mutexes used. This variant is worth noting because of the threat actor's prevalence, compromising over 100 organizations per month using BabyLockerKZ. In recent times, the group has been seen primarily targeting South American countries but has also targeted countries across the globe.[xi]
Bad Actors Try Out a New Tool	Forcepoint's X-Labs research team has helped shed light on a legitimate tool being abused to push AsyncRAT malware.	The legitimate "TryCloudflare" tool is used by developers to implement Cloudflare tunnel on a trial basis without registering with Cloudflare's DNS service. This can easily be used for malicious remote access anonymously. The technique was used in a campaign that kept AsyncRAT relatively the same, other than its exploitation of search-ms, a Windows search feature that is abused to download AsyncRAT from the TryCloudflare tunnel. To initiate contact, the adversaries reached their victims through phishing emails that contained a malicious HTML file with a link that used search-ms to download the payload.[xii]
Vicious Vilsa Stealer Makes Its Debut	Cyfirma has confirmed the existence of a new information stealer that goes by "Vilsa Stealer."	Discovered on GitHub, this Python-based malware's goal is to capture information such as browser data, cookies, passwords, crypto wallets, Steam data, Discord data, Telegram data, and more for the financial gain of the stealer's creators. Some of the malware's more notable features include targeting browser extensions, adding itself to the victim's startup programs, terminating programs like debuggers and reverse engineering tools, anti-VM protections, and exfiltration capabilities.[xiii]
Yunit Stealer Utilizing Subtle C2 Methods	Cyfirma has exposed a new information stealer that is named "Yunit Stealer."	Made in JavaScript, Yunit Stealer covers many tactics used by adversaries, such as persistence, defense evasion, collection, and exfiltration. For persistence, Yunit adds itself to the Windows registry run keys or the startup folder to open whenever the victim's device does. Yunit's defense evasion capabilities will hide malicious running windows along with modifying registry keys. The malware's collection features assemble locally stored data such as credentials, cookies, web browser autofill data, files, and application data. Finally, all collected data is exfiltrated to the attacker's C2 server through Telegram or Discord. No known threat groups have known

		connections to this malware, and it has not been seen used in the wild yet.[xiv]
Double Trouble	Unit 42 researchers have unearthed two new pieces of malware from the North Korean APT group Kimsuky.	The first, dubbed "KLogEXE," is a novel keylogger written in C++ by Kimsuky. Some of the information it collects includes running applications, traditional keyboard keylogging using GetAsyncKeyState, and mouse clicks. The second is a new undocumented variant of the FPSpy backdoor. Some of its features include stealing configuration data, downloading and running modules, C2 communication, command execution, and drive, directory, and file enumeration.[xv]
Taking Control with perfctl	Aqua Nautilus researchers have shared information with the public about a lesser-known piece of malware that has a multitude of capabilities, going by "perfctl."	This malware is known to target Linux-based servers to drop additional cryptomining and proxyjacking malware. The name perfctl comes from "perf," a Linux performance monitoring tool, and "ctl", meaning "control." Initial access to install perfctl starts with exploiting known Linux server vulnerabilities. Once exploited, the payload can be downloaded from the attacker's malicious HTTP servers. The malware also uses a backdoor for C2 communication purposes through TOR and rootkits to evade detection. The main goal of this malware is cryptojacking using the victim's hardware without their knowledge or consent.[xvi]
Horus Protector Protecting the Wrong People	The SonicWall threat research team recently discovered a new malware, "Horus Protector," known as a Fully Undetectable (FUD) crypter.	Horus Protector is used alongside other malware and is described as making your malware "undetectable." It "guarantees you optimal performance and longer persistence," according to discussions in the Horus Telegram group. Some of its features include file encryption, persistence capabilities, free updates, support from the Horus team, and more. In the latest version of Horus Protector, the malware uses the Windows registry to spread the additional malware. The Horus group also continues to update Horus Protector as protections for it are written.[xvii]
Malware Working Together	Zscaler has found a new connection between DarkVision RAT, PureCrypter, and the way they are delivered.	The malware itself has not changed, but its attack chain has. To start, a .NET executable is downloaded and decrypts a copy of Donut loader within itself, storing the loader in the victim device's memory. Donut loader then loads the third stage, containing PureCrypter. PureCrypter's main use is to decompress and deserialize DarkVision RAT, but it also features some useful defense evasion and persistence techniques to help with the installation. These include excluding DarkVision-related files in Windows Defender and injecting DarkVision RAT into running processes.[xviii]
Unusual Name Belies Skilled Capabilities in New Loader	Trustwave's threat intelligence team has found a new loader recently which goes by the name "Pronsis Loader."	This loader is noted to have similarities with D3F@ck Loader and has network infrastructure links to the developers of Lumma Stealer. Installation for Pronsis is noticeably different than D3F@ck however, with Pronsis using Nullsoft Scriptable Install System for installation and D3F@ck using Inno Setup Installer. Pronsis also differs from D3F@ck in its lack of signed certificates, making it easier to detect. Common payloads that were seen delivered with Pronsis are Lumma Stealer and Latrodectus.[xix]
The Sound of Silence	Trend Micro's threat hunting team has unearthed information about a novel red team tool, "EDRSilencer," being used maliciously.	The tool works by meddling with EDR solutions using the Windows Filtering Platform (WFP). It does so by blocking IPv4 and IPv6 communication between the network and the EDR solution through WFP filters, essentially taking the EDR offline. Its capabilities include scanning for running processes and either blocking all EDR traffic or blocking data transport to a

		specific process. EDRSilencer can target an array of EDR solutions such as Carbon Black, Cybereason, SentinelOne, Tanium, and more.[xx]
Forming a Warrior Band	The SonicWall Capture Labs threat research team researched and shared their findings regarding a new trojan with worm capabilities called “CoreWarrior.”	This worm functionality comes from CoreWarrior’s ability to spread across a network by generating copies of itself and communicating with multiple IP addresses, being able to open multiple sockets for backdoor access, and using Windows UI elements for monitoring. CoreWarrior is used to obtain data off victim devices and create hooks to watch command prompt for any modifications. The malware also has a few types of anti-analysis features, such as anti-debugging abilities, defense evasions using a randomized sleep timer, and VM detection. For data exfiltration, indicators in CoreWarrior’s code include mention of the use of FTP, SMTP, and POP3.[xxi]
Gotta Go Fast: ATM Targeting Remains a Viable Strategy	On a personal blog ran by X user @haxrob, the free agent exposed a new Linux variant of FASTcash malware, used to withdraw money from an ATM without authorization.	Compared to its previous Windows version, this Linux variant has less functionality, such as not having hardcoded IP checks or quality control as to how the card PIN is acquired. This version is written in C++ and is intended to accomplish initial access by injecting itself into running processes through ptrace. The malware is also responsive to ATM error codes, such as if the victim has insufficient funds or if the machine is reserved for ISO (Independent Sales Organization) use. All successful withdrawals have their cash converted to the Turkish Lira after successful theft.[xxii]
Flight of the Bumblebee Loader	The Netskope Threat Labs team has shown proof regarding a possible resurgence in Bumblebee Loader.	This time however, Bumblebee has changed their infection chain after the payload has been downloaded. To become stealthier in victim’s networks, Bumblebee now uses the Windows Installer SelfReg table instead of the previous CustomAction table which allowed the opportunity for victims to detect suspicious activity when a new process is created.[xxiii]
Crystal Rans0m Sports Modular Capabilities for Tailored Attacks	KrakenLabs threat intelligence team published a new headline regarding a ransomware family called “Crystal Rans0m.”	This lesser-known family is interesting in that it has both ransomware and information stealer abilities, allowing for attackers to not only encrypt files for ransom but also steal them beforehand. This permits the attackers to double their money by not only threatening the victim with losing their files, but also having them published online. In total, before encryption, Crystal Rans0m will gather data on all browser passwords, search history, downloads, visited sites, cookies, along with Discord tokens, Steam files, Riot files, and other data. KrakenLabs has also recently realized that Crystal Rans0m is likely a modular solution, only deploying what is necessary for the planned attack. It also now has the new addition of anti-VM measures, such as searching running processes for VM software.[xxiv]
Watch out for Ghosts this Halloween	Elastic Security Labs has brought malware updates to the GHOSTPULSE family to the public.	These updates have changed GHOSTPULSE to use pixel structures in PNG images, rather than IDAT chunks. As part of this development, the malware now assigns a value to each pixel based on its RBG value and can form a byte array containing the payload within a PNG. Previously, GHOSTPULSE was in separate parts, requiring assembly post-compromise. Now, it is included in a single executable and one PNG file. Interestingly, the phishing method used in this campaign is also unique, getting the victim to open the Run windows and paste a command they did not know they copied from the attacker-controlled website.[xxv]

The 007 of RATs	ThreatMon has detected a new RAT which they have named “X-ZIGZAG RAT.”	This trojan is interesting due to its stealthy qualities, such as running completely fileless in RAM, anti-VM detection, anti-AV detection, and its self-destruct function which can erase all traces of itself from a device. The malware is often delivered through phishing and remains in the system using Windows Task Scheduler. The data this RAT steals include system information, browser passwords, cookies, Wi-Fi credentials, and browser credit card information. This data is then sent to the attacker’s C2, which uses Base64 encoding and HTTP to avoid detection.[xxvi]
Feel the ‘Power’ of this RAT	Cisco Talos recently made a discovery from a suspected Russian threat actor revolving around a new piece of malware called “PowerRAT” by the company.	PowerRAT’s attack chain is as follows. First, a malicious link in a phishing email is sent to a victim. This link reaches out to an attacker-controlled server and downloads a malicious Word document containing PowerRAT. This Word document has a malicious Visual Basic macro within it which contains an encoded copy of a malicious HTA file and PowerShell loader. The macro then drops the decoded contents of the malicious HTA file to “UserCache.ini.hta” and the PowerShell loader into “UserCache.ini” in the victim machine's current user profile folder. UserCache.ini.hta then drops a JavaScript file that can be used to execute UserCache.ini, which leads to PowerRAT infection. The attackers also utilize Windows registry keys to automatically launch the malware when a victim logs in. PowerRAT will then activate, perform reconnaissance, collect sensitive data, and exfiltrate it back to the attacker’s C2 instance.[xxvii]
Clearly Fake WordPress Plugins	The GoDaddy security team recently made a fresh discovery of a new ClearFake variant.	In recent attacks using ClearFake, adversaries will first initiate action by logging into WordPress websites with stolen administrator credentials and then install fake plugins. These plugins contain malicious JavaScript that when executed in a web browser, present the victim with fake browser update notifications that tell them to unknowingly install information stealers on their devices. The most recent variant’s attack flow starts with a POST request to wp-login.php, the main login page of administrators for WordPress websites. After successful login, the attacker will open the “Add Plugins” page, upload a fake plugin, activate it, and reload the Plugins page.[xxviii]
Qilin’s New Look	Halcyon researchers have acknowledged a new Qilin ransomware variant they have dubbed “Qilin.B.”	This new Qilin variant written in Rust features many improved TTPs, such as AES-256-CTR or Chacha20 encryption and RSA-4096 with OAEP padding to protect the attacker’s encryption keys, making decryption impossible without the private key. This new version will also disable any security, backup or virtualization services, such as Veeam, Sophos, and SAP. Qilin.B can further delete volume shadow copies as well, preventing backups from being made. For defense evasion, not only can Qilin.B clear Windows Event Logs but also delete itself after it is no longer used. It can likewise enable persistence using autorun registry entries. This is only a fraction of the malware’s new capabilities.[xxix]
Evasive Panda Scouts the Skies	ESET researchers have investigated a previously unseen post-compromise toolset used by the Chinese APT group Evasive Panda named “CloudScout.”	CloudScout, written in C#, was originally seen being used against religious and government entities within Taiwan. CloudScout is a .NET malware framework that is made up of different modules that can be used to steal data from different cloud services, such as Google Drive, Gmail, and Outlook. It is employed as an extension to MgBot, another of Evasive Panda’s known malware frameworks, and uses a pass-the-cookie technique to hijack authenticated sessions from web

		browsers. After successful compromise, Evasive Panda will deploy a Nightdoor implant, which is a backdoor that functions off public cloud services for C2 communication. The name CloudScout was given to the malware by ESET from the PDB paths of the said modules including the text “CloudScout”.[xxx]
Unwelcome CAPTCHA Impersonators	Kaspersky has shed light on a new method of distributing malware, fake CAPTCHAs in ad networks.	Ad networks are essentiality middlemen, bringing together online advertisers and publishers where advertisers pay publishers to host their ads. The attack can work in multiple ways; for instance, some of the fake CAPTCHAs prompt visitors to scan a QR code, others instruct the user to run PowerShell after unknowingly copying and pasting malicious commands from the CAPTCHAs, with some persuading the visitors to do so with fake error messages as well. In these attacks, Kaspersky has seen the unknown adversaries installing Lumma Stealer or the Amadey trojan as the attacker’s end goals.[xxxi]
A Midnight Connection	Microsoft threat intelligence has recently seen APT29, also known as Midnight Blizzard, performing a mass phishing campaign utilizing a RDP configuration file to gain initial access, which is a new technique for the group.	Once the file is opened it connects to the attacker’s server and charts the victim’s device information to their server. This can include data such as disk drives, the clipboard, printers, IoT devices, audio software, Windows authentication features, and more. Furthermore, once an RDP connection is established, APT29 can install further malware such as RATs and map network shares. So far, this attack has been against those in government, academia, defense, non-governmental organizations, and other sectors, particularly in the United Kingdom, Europe, Australia, and Japan.[xxxii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Unlocking the Mysteries of Key Group	Kaspersky has compiled evidence of an under-observed threat group known as "Key Group" or "keygroup777." This financially motivated ransomware group is known to target Russian individuals. Key Group does not create their own custom ransomware and instead develops variants based off previously existing ransomware strains, such as Xorist, Chaos, Annabelle, Slam, UX-Cryptor, Hakuna Matata, Judge/NoCry, and more. The most recent variant used is NoCry, which encrypts files using AES-256-CBC and adds a "Keygroup777tg" extension. The encryption key used is made based on the victim's system data and sent to Key Group's C2 server in plain text, allowing stolen files to be decrypted without action from Key Group. Kaspersky suspects that Key Group is likely a subsidiary project of the Russian-speaking closed "huis" group due to Key Group's previous ransomware variants branding encrypted files with a "huis_bn" extension. The huis group is currently inactive and has been rebranded, showing a dated connection to the group.[xxxiii]
Stonefly Continues Targeting U.S. Organizations for Financial Gain	Symantec's threat hunter team has discovered three new attempted victims of the North Korean threat group, Stonefly. All these victims were private companies attacked in August and based in the United States with no known intelligence connections, showing clear financial motivation. In these attacks, Stonefly failed to install any malware or ransomware but displayed some recently discovered IoCs that were previously tied to Stonefly. The group also was seen using a fake Tabluea certificate signed by "Microsoft," a relatively new method for them., [xxxiv]
New CeranaKeeper Threat Group Pumps out the Malware	ESET researchers noticed new malicious activity starting in 2023 against government institutions in Thailand and have decided to make it a new threat actor, calling the group "CeranaKeeper." They chose this name because of the common string "[Bb]ectrl" in their toolset, with CeranaKeeper being a combination of beekeeper and the Asian honeybee's binomial name *apis cerana*. The group is believed to be based in China and likely state-sponsored due to its motivations of espionage. After making it onto a victim's device and installing the TONESHELL backdoor, CeranaKeeper continues to add malware to the machine, but of their own creation. The first found was "WavyExfiller," a Python package named after the WAV format it uses, used mainly for sending and receiving files from CeranaKeeper's Dropbox. Second was "DropboxFlop," a reverse shell with additional download and upload features. Third was "OneDoor," a C++ backdoor that abuses OneDrive's REST API for Microsoft Graph API. Finally, the piece of malware found was "BingoShell," a Python backdoor that uses GitHub for C2 purposes.[xxxv]
Lifting the Veil on SHROUDED#SLEEP	The Securonix Threat Research team published their findings on a new active campaign, which the team has named "SHROUDED#SLEEP" and attributed to North Korea's APT37. The aim of the campaign is to install a PowerShell backdoor/RAT which is called "VeilShell." Some of VeilShell's features include listing file details, zip and unzip files, upload, download, modify, or delete files, create or modify registry keys, schedule tasks, and exfiltration through a CSV file to the attacker's server. Distribution of VeilShell starts with a phishing email being delivered with a ZIP file attached containing a malicious double extension file (*.xlsx.lnk) containing PowerShell that drops and executes files until eventually the VeilShell PowerShell can run. So far, Cambodia has been the sole target of these attacks, but due to APT37's record, it can easily extend to other Southeast Asian countries as well.[xxxvi]
GoldenJackal's Blinged Out New Toolbox	ESET researchers have neatly summarized the current toolset of the GoldenJackal APT group, including the addition of new tools. Named by ESET, these new pieces of GoldenJackal malware are called the following: "GoldenDealer," "GoldenHowl," "GoldenRobo," "GoldenUsbCopy," "GoldenUsbGo," "GoldenAce," "GoldenBlacklist," "GoldenPyBlacklist," "GoldenMailer," and "GoldenDrive." To go down the list,

	GoldenDealer is malware that allows executables to be delivered to non-Internet connected devices though USB drives. Next, GoldenHowl is a Python backdoor with additional modules for added capabilities. Third up is GoldenRobo, which collects files on a victim's device and exfiltrates them back to GoldenJackal. Following that is GoldenUsbCopy and GoldenUsbGo, used for monitoring the use of USB drives, along with copying files to later be exfiltrated, with GoldenUsbGo simply being an updated version of GoldenUsbCopy. Similarily to the other malware listed here, GoldenAce is used to continue to transmit other malware and retrieve further malicious payloads through USB drives. GoldenBlacklist and GoldenPyBlacklist process emails and store those of interest, with GoldenPyBlacklist simply being the Python version of GoldenBlacklist. GoldenMailer, on the other hand, uses email to send bundled, sensitive information through email attachments back to GoldenJackal. Finally, GoldenDrive, which does a similar job to GoldenMailer, but instead uploading the stolen data to Google Drive.[xxxvii]
Cyber Critters Deploy BeaverTail, InvisibleFerret Malwares	Unit 42 has continued to follow the CL-STA-240 Contagious Interview campaign that they first published news about in 2023. They now wish to update the public on two new variants of the malware used in this campaign, "BeaverTail" and "InvisibleFerret." BeaverTail is a downloader and infostealer which, in this newest version, has been written in Qt rather than JavaScript, allowing BeaverTail to target both Windows and macOS devices equally. However, most features stay the same, except for two new capabilities: cryptocurrency theft for both Windows and macOS and browser password theft for macOS. For InvisibleFerret, fewer changes were made, with there being only slight improvements. Unit 42 notes this as important, however, as it shows the malware is still being updated. Unit 42 also believes that the campaign aligns with North Korean interests, implying a nation-state actor is involved.[xxxviii]
New Moon, New Loader	BI.ZONE Threat Intelligence has uncovered a new loader and technique used by the threat group Core Werewolf. The loader, written in AutoIt, has many capabilities, including gathering system information data; creating, renaming, moving, and opening files; directory and file enumeration; and exfiltrating captured data to Core Werewolf's C2 servers through HTTP POST requests. It can also pull-down further payloads from the C2, such as further AutoIt malware. Their new method of malware delivery is Telegram, along with their previous methods of phishing.[xxxix]
Into the Hive Targeting Latin America	IBM X-Force has updated the public with their findings on Hive0147, a cyber criminal organization which originates from Latin America. The group is targeting financial institutions and is known for distributing various banking trojans such as Mekotio and Banker.FN. Recently, however, Hive0147 has been seen using a new, custom, Golang-based downloader, which goes by "Picanha." Picanha is first delivered through phishing, with the phish containing a link to a zipped copy of Picanha. The loader has a choice of 10 recorded Hive0147 domains to pull further payloads from. It also checks for traces of the Topaz OFD banking security protection module. The main goal of the current campaign using Picanha is to deliver Mekotio to their victims.[xl]
EvaLUAting the Growth of Lua Malware	Morphisec Threat Labs has provided an update regarding the use of Lua malware variants targeting the educational sector, specifically educational video game services. This malware is advertised typically through SEO poisoning, with new examples being a website claiming to have a Roblox cheat engine to download. After hitting download, an initial ZIP file is pushed from the attacker GitHub to the victim. Lua then splits into four files: a DLL file used as a runtime interpreter for Lua, an executable that functions as a loader to load the previously mentioned DLL, a Lua script containing the malware, and a batch script used to help run the executable. The Lua malware process functions by receiving victim data and sending commands from the attacker's C2 instance for additional payloads to be downloaded. Changes seen in Lua include a simplified delivery of Lua malware, along with the malware now using obfuscated Lua scripts instead of previously used compiled Lua bytecode.[xli]
Embargo Group Gets an Upgrade	ESET researchers' investigation led to the discovery of a novel Rust-based toolkit created by the Embargo ransomware group. The new toolkit contains a loader called "MDeployer," meaning "EMbargo Deployer," and an EDR killer named "MS4Killer," both named by ESET. MDeployer is the main method for facilitating loading all further malware onto victim machines. Currently, there are two MDeployer versions, one in an

	executable format and one in DLL format, likely to attempt to avoid detections by abusing Windows Safe Mode. The loader is also capable of cleaning artifacts such as leftover MS4Killer files. MS4Killer on the other hand, meaning "EMbargo s4killer," believed to be inspired by s4killer, is a defense evasion tool that is used to terminate security-related processes using the Bring Your Own Vulnerable Driver (BYOVD) technique. The driver Embargo is currently abusing is a minifilter driver called probmon.sys. The actions on objective of this toolkit are for the Embargo group to successfully deploy ransomware in a victim.[xlii]
This New Campaign is Charging Up	SEQRITE Labs APT-Team has unearthed a new campaign which the team is calling "Operation Cobalt Whisper." While the aggressors are currently unknown, we do know that the group targets Hong Kong, China, India, and Pakistan, specifically industries such as defense, electrotechnical and environmental engineering, energy, civil aviation, academia and research institutions, medical institutions, and independent cybersecurity researchers. The attack chain starts with a ZIP archive delivereded in a phishing email containing a LNK file. This LNK file then uses wscript to run batch scripts that enable Cobalt Strike on the victim's device. A decoy document is then deployed to redirect the victim's attention, while the batch scripts are renamed and scheduled as tasks for persistence. Finally, the Cobalt Strike beacon reaches out to the attacker's C2 instance and exfiltrates any collected data.[xliii]
Black Basta Hops in a Teams Call	ReliaQuest has been on the hunt, investigating the social engineering tactics of the Black Basta ransomware group. In October, the group changed their modus operandi in multiple ways, with the main being the use of Microsoft Teams. Within Teams, Black Basta would add targeted victims to Teams chats and pretend to be an administrator or help desk personnel. Victims were also sent QR codes within these chats that link to malicious domains, camouflaged as legitimate QR codes from a real company. The goal of Black Basta in these attacks is to install remote monitoring and management (RMM) tools for initial access, where they have traditionally used AnyDesk for this reason. However, ReliaQuest found that Black Basta is now using QuickAssist for RMM and not solely AnyDesk, expanding their toolset. The ransomware group seems to continue to perform their previous choice of social engineering as well, sending large amounts of spam emails to the victims and then vishing them, still pretending to work for a help-desk service.[xliv]
You Dun Messed Up, Leaves Toolset Exposed in Open Directory	The DFIR Report's Threat Intel Team discovered an open directory belonging to a Chinese threat group calling themselves "You Dun." This group has been seen targeting countries like South Korea, China, Thailand, Taiwan, and Iran but has no industry it prefers to target. In this open directory, DFIR Report analysts were able to uncover what is believed to be the group's entire toolkit. Going down the list starting with reconnaissance-based malware, You Dun uses WebLogicScan, Vulmap, Xray, and dirsearch. For initial access, they used Sqlmap, Seeyon_exp, and Weaver. Command and Control is run by Cobalt Strike, Ladon, and Viper. Next, privilege escalation is achieved using CDK and Traitor. From DFIR Report's investigation, it appears the group's end goal is to install a custom LockBit variant on their victims' devices for ransom.[xlv]
The HeptaX Vex	Cyble Research and Intelligence Labs encountered a new threat actor campaign which they are dubbing "HeptaX." The attack chain starts with a ZIP archive attached to a phishing email. This ZIP file contains an LNK file which executes PowerShell commands to download and execute malware from the attacker's server, such as phishing lures, PowerShell, batch scripts, and ChromePass, a password recovery tool. The scripts work together to create a new administrator account and modify RDP settings. The goal of the HeptaX campaign is likely to establish RDP access to a victim's device, which would allow the attackers to exfiltrate data, install more malware, or perform discovery on the affected device.[xlvi]
TeamTNT's Campaign Plans Blow Up in Their Faces	Aqua Nautilus researchers have taken notice of preparations being made for a new campaign run by TeamTNT, an established cybercriminal group. How this developing campaign is likely to go is by TeamTNT first exploiting internet-facing Docker daemons on ports 2375, 2376, 4243, and 4244 using a custom script TeamTNT has created called the "Docker Gatling Gun." This is used to target IP addresses in mass and automatically deploys a container from TeamTNT's compromised Docker Hub account.

	The group then deploys two docker containers, one that allows for the victim's devices to be rented out as cryptocurrency mining resources for shady customers and another that facilitates further persistence and command and control over the victim's devices. Some of the actions this container performs include adding itself to a Docker Swarm to avoid detection, installing a payload of the Sliver C2 framework, and a scanner tool that looks for further vulnerable Docker daemons to exploit.[xlvii]
Tenacious P Emerges from North Korea	Datadog Security Research has connected the dots between the campaign "Contagious Interview" and a new threat actor Datadog has designated "Tenacious Pungsan." The name was chosen by Datadog because Pungsan is a dog native to North Korea, where the group is located. In the group's recent attacks, they have used npm packages that contain BeaverTail, which is JavaScript malware designed to steal information and load further stages of malware. What makes BeaverTail interesting in this case is its ability to link Tenacious Pungsan and Contagious Interview with its shared use of a new Qt GUI variant of BeaverTail only seen in Contagious Interview campaigns. In addition, the group and campaign have been seen sharing resources, such as IPs and web directory structures, further establishing their connection.[xlviii]
Andariel Needs to Stop Playing Around, Links to Ransomware Observed	Unit 42 has taken special note of changes in the North Korea-based threat group, Andariel. During their investigation, Unit 42 discovered that Andariel gained initial access through a compromised user account and followed with lateral movement and persistence techniques provided by Sliver and their own custom malware, DTrack, to other devices through SMB. Sliver and DTrack were also used for C2 communication, which ultimately led to the deployment of Play ransomware, with its use being a never-before-seen application of existing ransomware by Andariel for the first time. It is believed that there have been no changes made to Play by Andariel either.[xlix]

Dark Web Markets

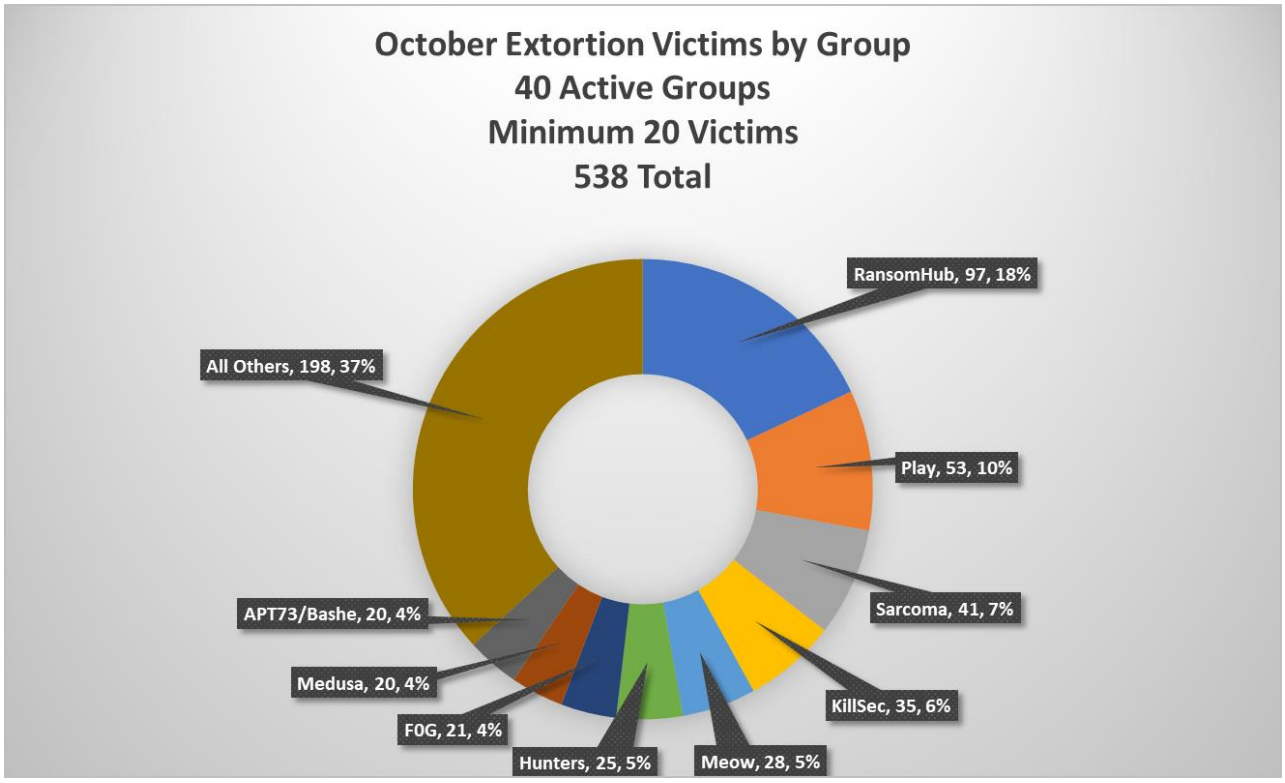
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

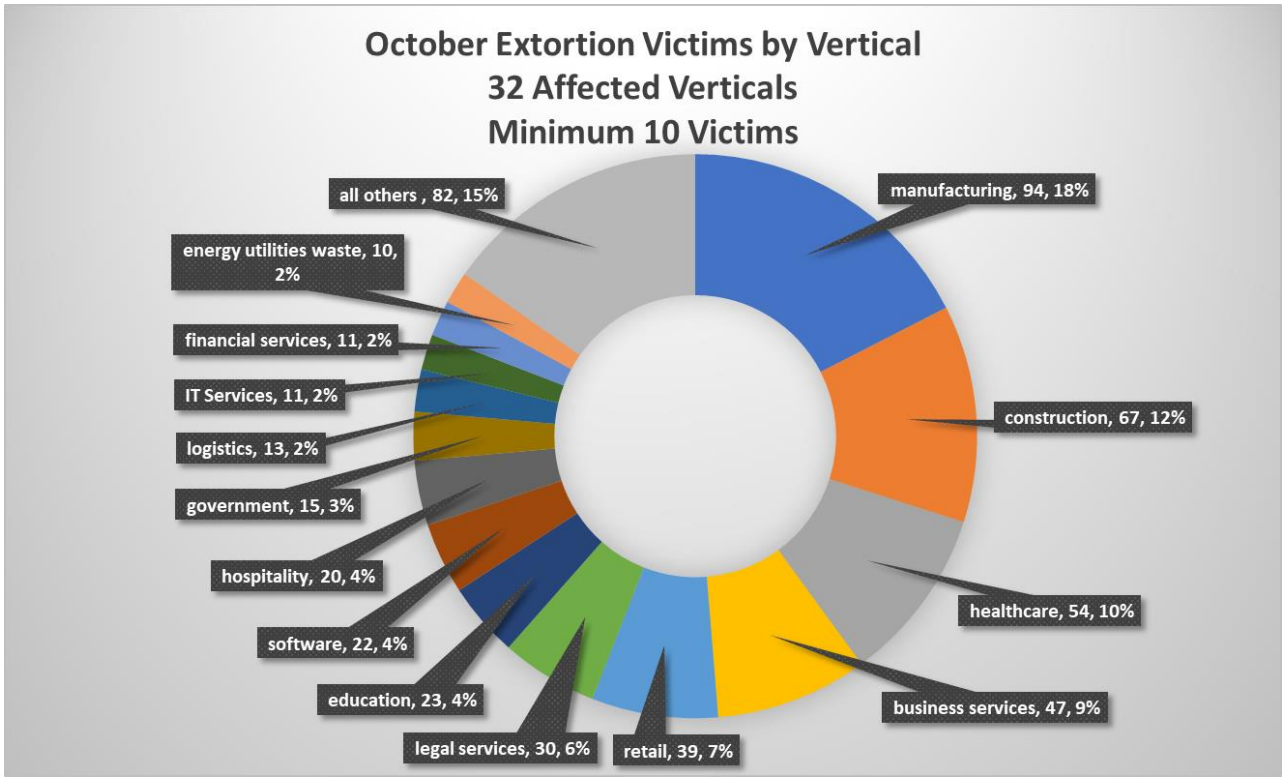
Activity	Note
Actor Developments	DragonForce ransomware released an updated version of their ransomware, writing: Dear partners, We'd like to present the latest update to our system which will take your possibilities to a completely new level and significantly optimize the work process. Key improvements: • Multibuild. Now you can work on up to six builds with one client simultaneously in a convenient window. Support for multiple systems - Windows, Linux, ESXi, NAS. • Expansion of NAS support. Complete support for a NAS locker in UNIX systems. Successfully tested on FreeBSD.
Access Sale	An access broker was observed selling SMB and domain user Cisco VPN access to an Australia-based minerals and mining company with USD 6.9 billion in revenue for USD 8,000. He said the antivirus was "unknown."
Access Sale	An access seller was observed selling domain user SMB access to a U.S.-based transportation company with USD 290 million in revenue for USD 1500.
Actor Developments	In a wide-ranging investigation involving law enforcement in more than a dozen countries, the United States Department of Justice and the British National Crime Agency announced charges and arrest of members of the LockBit ransomware organization and the operators of Cryptex and UAPS, major money laundering operations catering to Russian cyber criminals. Shockingly, Russian authorities also opened an investigation into Cryptex and UAPS and made around 100 arrests, including people indicted and sanctioned by the United States. On 26 September, the United States unsealed charges against Russian national Sergey Ivanov for operating money laundering and illicit cryptocurrency exchange sites. Ivanov, known online as “Taleon” among other aliases, was accused of laundering more than USD 1 billion in illicit transactions since 2013 via operating exchange services Cryptex, UAPS, PinPays, and PM2BTC. These sites laundered proceeds from the Rescator and Joker’s Stash stolen credit card sale sites, among other criminal enterprises. Additionally, Timur Shakhmametov, a 20-year cyber crime veteran, was accused of operating the Joker’s Stash site. Between 2014 and 2021, the Joker’s Stash site may have sold up to USD 1 billion in stolen credit cards from dozens of major point-of-sale breaches. On 2 October, the Russian authorities announced an investigation into Ivanov and reportedly raided his house. In all, authorities announced around 100 arrests across the country. The reasons behind Russia’s actions are mysterious. Until now, Ivanov and his associates have operated with apparent impunity. The Russian actions have unnerved many in the Russian language cyber crime community, as their services were widely used.
Actor Developments	On 30 September, the UK National Crime Agency reactivated the LockBit sites that they had seized earlier this year and posted more information related to the LockBit gang. They named Aleksandr Ryzhenkov, a high-ranking member of the Russian intelligence linked Evil Corp, as being a prominent member of LockBit. The press releases by the US DOJ and the Department of Treasury’s Office of Foreign Asset Control (OFAC) highlighted Ryzhenkov’s ties to Maksim Yakubets, the leader of Evil Corp, who in turn is related to the former head of the Federal Security Service (FSB) Vympel special forces unit. Yakubets was also said to have business ties with the current head of the FSB Special Purpose Center Aleksandr Tikhonov, a deputy Chief of Staff of the Presidential Administration Dmitry Kozak, and Herman Gref, the CEO of the largest bank in Russia, all of whom are also under US sanctions.
Access Sale	An actor sold access to a U.S.-based manufacturing company with more than USD 615 million in revenue for USD 2,000.

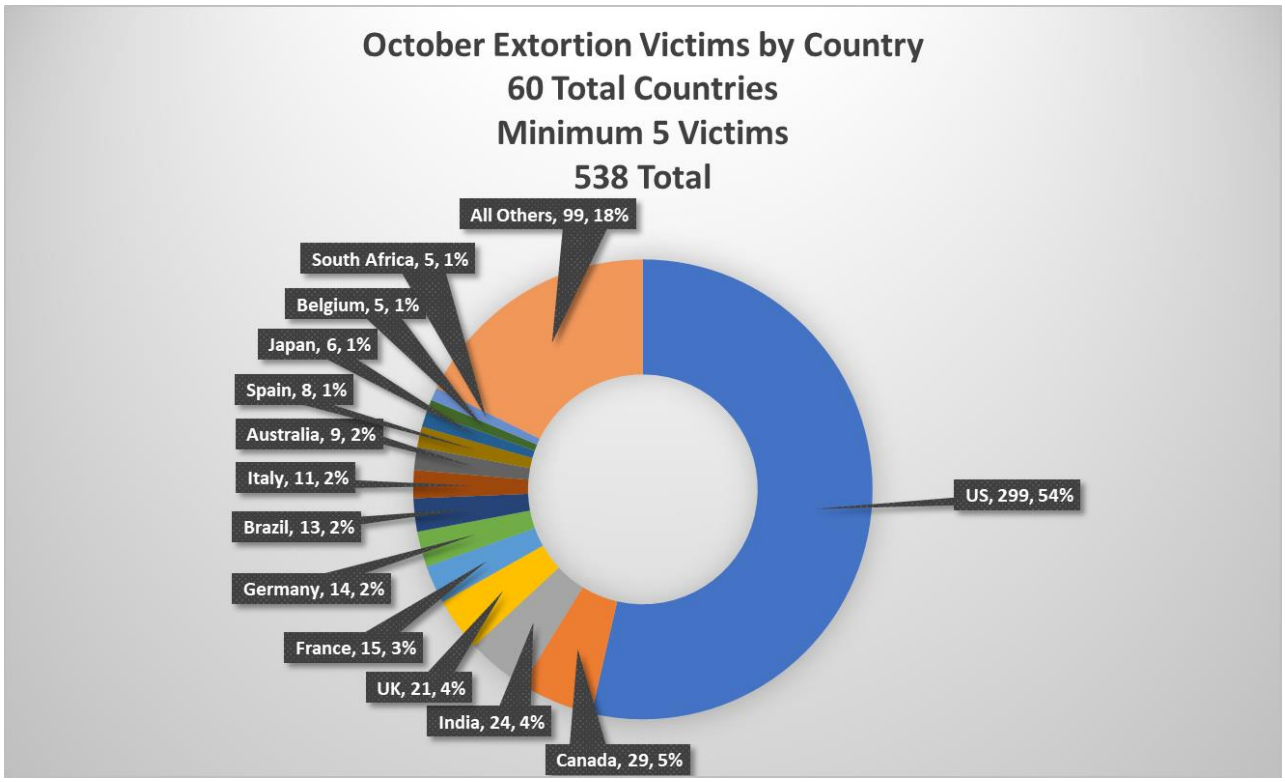
Access Sale	An actor was observed selling domain user access to an unnamed business services company with USD 173 million in revenue for USD 1,500.
Data Sale	An actor was observed selling two million records stolen from Thomasville, GA based Senior Life Insurance Company.
Data Sale	An actor was observed selling what they claimed was customer data belonging to a “credit scoring company – a major player with its own score technique” and “a major influence in the financial industry” with around USD 2 billion in revenue.
Access Sale	An access seller sold Fortinet domain admin access to a U.S.-based luxury hotel with USD 50 million in revenue and 400 employees for USD 2,000.
Access Sale	A new actor attempted to sell RDP access to an Irish company offering insulation and building envelope solutions with USD 9 billion in revenue but lost access before completing the sale.
Access Sale	An actor was observed selling Citrix RDP access to a U.S.-based networking software company with USD 3.3 billion in revenue for USD 1,500.
Data Sale	A notorious actor posted multiple documents stolen from Cisco and released a list of Cisco customers supposedly impacted by the breach. Cisco confirmed that their public facing DevHub was probably compromised and shut down access.
Access Sale	An actor was observed selling VPN access to a Colorado-based enterprise in the automotive service and collision repair business with USD 51.2 million in revenue for a buy now price of USD 2,500.
Access Sale	An actor on multiple crime forums sold VPN admin access to an unnamed U.S.-based non-profit health center with between USD 20 - 50 million in revenue and more than 415 hosts for USD 2,000. The first response to the sale offer was, "No conscience. Make sure he pays a security deposit," and the second response was in English and echoed those sentiments.
Access Sale	An actor was observed selling VPN access to a U.S.-based ISP and cable TV provider with between USD 10 and 30 billion in revenue (posted as USD 15 billion in the title of the post) for USD 3,000. The actor described the company as "one of the largest providers of cable TV and internet and offering internet services to large companies. The VPN allows access to the servers of these companies and also a number of virtual machines and other networks. This is suitable for a supply chain attack."
Data Sale	An actor was observed selling data on 350 million customers belonging to Hot Topic, Torrid, and BoxLunch. The data supposedly included the rewards database, the emails database, and limited credit card details (name, last four, expiration). Price was USD 20,000.
Access Sale	An actor was observed selling access to the cloud environment of "a leading company known for its transformative intelligence." He claimed that the revenue is over USD 2 billion. His asking price was 3 BTC (~$195,000).
Access Sale	An actor was observed selling access to a university based in California for USD 700 with USD 253.8 million in revenue.

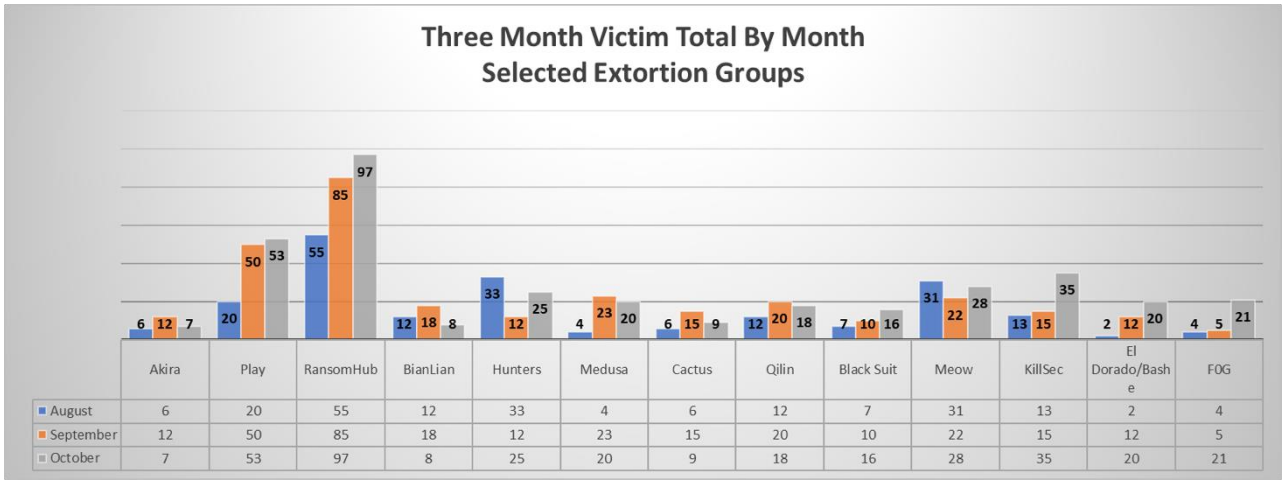
By The Numbers

Summarizing incidents in graphical format

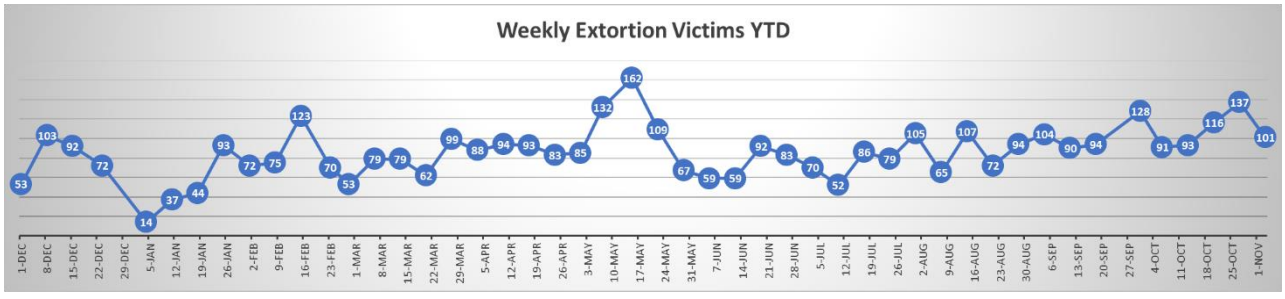








	Akira	Play	RansomHub	BianLian	Hunters	Medusa	Cactus	Qilin	Black Suit	Meow	KillSec	El Dorado/Bash e	F0G
August	6	20	55	12	33	4	6	12	7	31	13	2	4
September	12	50	85	18	12	23	15	20	10	22	15	12	5
October	7	53	97	8	25	20	9	18	16	28	35	20	21



New Detection Content

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

- **O365 Activity from High-Risk Country**
    a. This analytic triggers on any O365 activity originating from the following high-profile countries: Belarus, Cuba, Iran, North Korea, Russia, North Sudan and South Sudan, Syria, and Ukraine.

- **Google Cloud SCC: Cloud IDS**
    a. This analytic alerts on Google Cloud Security Command events that are detected by Cloud IDS. Cloud IDS detects layer 7 attacks by analyzing mirrored packets. It also includes command and control DNS tunnelling.

- **EDRSilencer EDR Disabling Tool**
    a. Looking for a malicious tool used to disable EDRs.

- **Google Cloud SCC: Lateral Movement Findings**
    a. This analytic alerts on Google Cloud Security Command Center lateral movement recovery detections. Examples of this activity include modifying boot disk attached to instances and OS patch executing from service account.

- **Google Cloud SCC: Impair Defenses / Inhibit System Recovery Findings**
    a. This analytic alerts on Google Cloud Security Command Center impair defenses or inhibit system recovery detections. Examples of this activity include disabling strong authentication, disabling two-step verification, and deleting Google Cloud backups, polices, or profiles.

- **Successful Azure AD Sign-in from High-Risk Country**
    a. This analytic triggers on any successful sign-in originating from the following high-profile countries: Belarus, Cuba, Iran, North Korea, Russia, North Sudan and South Sudan, Syria, and Ukraine.

[i] https://www.proofpoint.com/us/blog/threat-insight/security-brief-royal-mail-lures-deliver-open-source-prince-ransomware
[ii] https://regmedia.co.uk/2024/10/03/callistogroupwarrant.pdf
[iii] https://www.noticeofpleadings.com/starblizzard/
[iv] https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA==&mid=2247501270&idx=1&sn=203ae98a60ffc172cb9e06a1b95116c6&chksm=f9c1f6dfceb67fc916f29b04e9e63fe81a1f916d575ae8c32250fb954ca9619153ba864e118d&scene=178&cur_album_id=1955835290309230595
[v] https://www.trendmicro.com/en_in/research/24/j/fake-lockbit-real-damage-ransomware-samples-abuse-aws-s3-to-stea.html
[vi] https://securelist.com/miner-campaign-misuses-open-source-siem-agent/114022/
[vii] https://therecord.media/ransomhub-gang-behind-attack-mexican-airport-operator
[viii] https://news.cloudsek.com/2024/10/oilrig-cyber-attacks-apt34-targets-aerospace-sector-with-exploited-vulnerabilities-and-data-theft/
[ix] https://www.bleepingcomputer.com/news/security/free-frances-second-largest-isp-confirms-data-breach-after-leak/
[x] https://www.silentpush.com/blog/fin7-malware-deepfake-ai-honeypot/#FIN7-AI-Deepfake-malware-analysis
[xi] https://blog.talosintelligence.com/threat-actor-believed-to-be-spreading-new-medusalocker-variant-since-2022/
[xii] https://www.forcepoint.com/blog/x-labs/asyncrat-python-trycloudflare-malware
[xiii] https://www.cyfirma.com/research/vilsa-stealer/
[xiv] https://www.cyfirma.com/research/yunit-stealer/
[xv] https://unit42.paloaltonetworks.com/kimsuky-new-keylogger-backdoor-variant/
[xvi] https://www.aquasec.com/blog/perfctl-a-stealthy-malware-targeting-millions-of-linux-servers/
[xvii] https://blog.sonicwall.com/en-us/2024/10/horus-protector-part-1-the-new-malware-distribution-service/
[xviii] https://www.zscaler.com/blogs/security-research/technical-analysis-darkvision-rat
[xix] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pronsis-loader-a-jphp-driven-malware-diverging-from-d3fck-loader/
[xx] https://www.trendmicro.com/en_us/research/24/j/edrsilencer-disrupting-endpoint-security-solutions.html
[xxi] https://blog.sonicwall.com/en-us/2024/10/corewarrior-spreader-malware-surge/
[xxii] https://doubleagent.net/fastcash-for-linux/#detection-and-prevention
[xxiii] https://www.netskope.com/blog/new-bumblebee-loader-infection-chain-signals-possible-resurgence
[xxiv] https://outpost24.com/blog/crystal-ransom-hybrid-ransomware/
[xxv] https://www.elastic.co/security-labs/tricks-and-treats
[xxvi] https://threatmon.io/blog/x-zigzag-rat/
[xxvii] https://blog.talosintelligence.com/gophish-powerrat-dcrat/
[xxviii] https://www.godaddy.com/resources/news/threat-actors-push-clickfix-fake-browser-updates-using-stolen-credentials
[xxix] https://www.halcyon.ai/blog/new-qilin-b-ransomware-variant-boasts-enhanced-encryption-and-defense-evasion
[xxx] https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services
[xxxi] https://securelist.com/fake-captcha-delivers-lumma-amadey/114312/
[xxxii] https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
[xxxiii] https://securelist.com/key-group-ransomware-samples-and-telegram-schemes/114025/
[xxxiv] https://symantec-enterprise-blogs.security.com/threat-intelligence/stonefly-north-korea-extortion
[xxxv] https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/
[xxxvi] https://www.securonix.com/blog/shroudedsleep-a-deep-dive-into-north-koreas-ongoing-campaign-against-southeast-asia/
[xxxvii] https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/
[xxxviii] https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/
[xxxix] https://bi-zone.medium.com/core-werewolf-hones-its-arsenal-against-russias-government-organizations-7fbe8cc58b27
[xl] https://securityintelligence.com/x-force/hive0147-serving-juicy-picanha-with-side-of-mekotio/

[xli] https://blog.morphisec.com/threat-analysis-lua-malware
[xlii] https://www.welivesecurity.com/en/eset-research/embargo-ransomware-rocknrust/
[xliii] https://www.seqrite.com/blog/operation-cobalt-whisper-targets-industries-hong-kong-pakistan/
[xliv] https://www.reliaquest.com/blog/black-basta-social-engineering-technique-microsoft-teams/
[xlv] https://thedfirreport.com/2024/10/28/inside-the-open-directory-of-the-you-dun-threat-group/
[xlvi] https://cyble.com/blog/heptax-unauthorized-rdp-connections-for-cyberespionage-operations/
[xlvii] https://www.aquasec.com/blog/threat-alert-teamtnts-docker-gatling-gun-campaign/
[xlviii] https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/#key-points-and-observations
[xlix] https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/