Monthly Threat Intelligence Rollup

DEEP seas

TLP:CLEAR

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Chrome and Edge Extend Their Attack Surfaces	The ReasonLabs Research Team has released details about a surge of malicious browser extensions which are being forcefully installed onto Windows devices without permission, affecting at least 300,000 Google Chrome and Microsoft Edge users. This process begins with the victim downloading a malicious executable from a fake downloader website that appears to offer a legitimate service. After installation, the executable then registers a scheduled task using PowerShell written to the system32 folder, which downloads a payload from the attacker's C2 server. This payload is an installer that creates a new directory at "C:\Windows\NvOptimizerLog," where the rest of the malicious files used by the attackers will be held. Another PowerShell script is then executed, adding registry values for the malicious extensions to force their installation for the browser store, disabling future browser updates and enabling further communication with the attacker's C2. Another local extension is then downloaded to "C:\Windows\InternalKernelGrid," which has many capabilities, including interception of all web requests, hijacking search queries to move traffic through the attacker's servers, C2 communication, storage access, remote command capabilities, and encrypted scripts that can be injected or loaded into webpages.[i]
Seeing Double with UULoader	Last month the Cyberint Research Team noted an increasing trend in the use of a novel installer, masquerading as legitimate programs, which was targeting Korean and Chinese speakers. This installer, named UULoader after its embedded file paths, is likely to originate from China and has a straightforward execution sequence. To start, the victim opens an MSI file that contains additional files, such as a decoy file, UULoader itself, the final payload, and other supporting files. One of these supporting files is a VBS script, which when executed, adds headers to the other important files, such as UULoader itself, using a method called file header stripping, which is used to evade detection. Following this, a copy of Realtek.exe from the MSI file executes, sideloading UULoader, which later loads the final payload. The final payload is usually a well-known tool such as Gh0stRat or Mimikatz, the former of which is predominantly utilized by Chinese nation-state actors.[ii]
A Shift in the EDR Killer Tool Market	Sophos revealed data about the new "EDRKillShifter" tool has recently made it to the public eye. EDRKillShifter is a new malware loader designed to terminate endpoint protection software, which is currently believed to be used by the threat actors behind RansomHub ransomware. The loader functions by first running a command line with a password that allows for an embedded file on the victim to be decrypted and run in memory. This embedded file unpacks and executes a payload that installs from a selection of legitimate insecure drivers to gain the privileges needed to disable an EDR's protection. Sophos also suggests that EDRKillShifter may have not been developed by the RansomHub operators but instead purchased from dark net forums. This has not been confirmed yet. Internal review of the provided indicators of compromise corroborates the claims of links to the RansomHub group.[iii]
BANSHEE Stealer Makes Its Presence Known	Elastic Security Labs performed an extensive analysis on the recently revealed "BANSHEE" infostealer. BANSHEE Stealer is written in C++, targets macOS, and pursues sensitive system information, browser data, and cryptocurrency wallets. Similar to other stealers like AgentTesla, it is being marketed by its creator on the dark web and sold on a subscription basis to other would-be hacking groups. The

	stealer also features other sophisticated aspects, including anti-debugging and anti-VM protection, language checks, data collection, password phishing, encryption, directory creation, compression, and exfiltration, to name a few. BANSHEE also works on a variety of browsers from Chrome and Firefox to Vivaldi and Yandex. Despite all these features, the malware has a noticeable lack of obfuscation, making it easy to see what is happening behind the scenes.[iv]
RansomEXX Aims Sights at India's Finance Sector	A recent ransomware attack by the RansomEXX group struck India's banking infrastructure, specifically banks and payment providers. They did so by exploiting CVE-2024-23897, a critical vulnerability in Jenkins versions 2.441 and earlier and LTS 2.426.2 and earlier. This exploit allows unauthenticated attackers to read arbitrary files on a Jenkins controller file system, allowing for secure shell access by reading private keys. In the case of Brontoo Technology Solutions, the victim in RansomEXX's attack, the attack was successful because port 22 of its Jenkins server being open. The final objective of the RansomEXX group was the installation of their RansomEXX 2.0 ransomware.[v]
Doppelgänger Campaign Shut Down by German Authorities	CORRECTIV, Qurium, and the Bavarian Office for the Protection of the Constitution (Germany's intelligence agency) have been hard at work since 2022 tracking a stealthy Russian propaganda campaign named "Doppelgänger." Doppelgänger is known as the largest Russian disinformation campaign known to date and spreads propaganda by impersonating legitimate western websites. So far, the campaign has been primarily directed against Germany with other countries falling victim to a lesser degree, including the U.S., France, and Ukraine. Recently, the campaign had their phishing websites reach 800,000 clicks within eight months, showing unfortunate success. Thankfully, Hetzner, the data center operator used by Doppelgänger, has since blocked their customer accounts. Further proof of Russian collusion noticed by CORRECTIV include use of the Russian Cyrillic alphabet, use of Russian IP addresses, and work and holiday schedules corresponding with Russian time zones and calendars.[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
Gh0stGambit Trips Up Chinese Chrome Users	eSentire informed the public of a new, evasive dropper, which TRU has named "Gh0stGambit".	The dropper has been seen being delivered through a malicious webpage serving a fake Google Chrome installer. While the actor behind this campaign is unknown, it is believed that this campaign is primarily targeted at Chinese Chrome users, based on the use of Chinese web lures and targeting Chinese applications for data theft. After installation, Gh0stGambit attempts to complete its goal of installing a Gh0st RAT variant on the victim's device. Some unique features of Gh0stGambit include AV evasion, C2 capabilities, persistence through Windows Registry, and hiding remaining artifacts.[vii]
Breaking Down BITSLOTH BIT by BIT	Elastic Security Labs released news about a newly discovered Windows backdoor which the team has dubbed "BITSLOTH".	The name BITSLOTH was given due to the malware using Microsoft's native Background Intelligent Transfer Service (BITS), which is used by programmers and system administrators to download files from or upload files to HTTP web servers and SMB file shares. BITS can be abused to push BITSLOTH since BITS is primarily used for software updates and treats all its traffic as trusted. Due to the volume of logging functions and strings written in Chinese, Elastic has attributed BITSLOTH authors to be Chinese, though attribution to a specific group or nation-state actor is unavailable at this time. BITSLOTH's capabilities include C2 communication, command execution, file transfers, enumeration, discovery, keylogging, screen captures, and more.[viii]
Oh Deer… Not Another Stealer!	The Any.RUN team recently released a report detailing a new malware distribution campaign which has been labeled "DeerStealer".	The DeerStealer group's mission is to spread malware and steal data through fake Google Authenticator websites. They do so by using Telegram bots to retrieve the victim's IP address and location and spread their custom DeerStealer information stealer. The stealer, written in Delphi, has a goal of dropping a payload in the victim's memory, whereupon data is exfiltrated via C2 communication. This data can range from basic system information to full file transfers. Due to similarities between the DeerStealer infostealer and another stealer called "XFiles," such as reused C2 domains, Any.RUN analysts believe that the DeerStealer infostealer is a modified version of XFiles. The DeerStealer group's motivations and country of origin are currently unknown.[ix]
OFBiz is Busy Causing Problems	Thanks to the SonicWall Capture Labs threat research team, new information has emerged regarding a critical vulnerability in Apache OFBiz, an open-source enterprise resource planning (ERP) system and a suite of business applications developed by the Apache Software Foundation.	This vulnerability, being tracked as CVE-2024-38856, has a CVSS score of 9.8 and is detailed as a method for unauthenticated remote code execution. This is done by manipulating the OFBiz methods "getRequestUri" and "getOverrideViewUri," causing their values to mismatch. Authentication checks are done by getRequestUri; thus, if getRequestUri has the opposite value it is supposed to, it allows for an attacker to submit a modified request for access to be approved. Thankfully, Apache has patched out this vulnerability for OFBiz. Upgrading an existing

	"OFBiz" stands for "Open For Business."	OFBiz instance from 18.12.14 or older to 18.12.15 or newer is all that is required to counter this threat.[x]
Hunters International Sharpens Up	The Quorum Cyber Incident Response team uncovered a new Remote Access Trojan (RAT) used by the crime syndicate Hunters International labeled "SharpRhino" by Quorum Cyber, due to its implementation language being C#.	The malware is distributed through fake Angry IP Scanner installer files, hiding malicious files behind password protected 7ZIP *.7z files. Though Angry IP Scanner is not malicious in and of itself, actors have been known to abuse it as part of their toolsets. Some notable qualities of SharpRhino include its capabilities of persistence, installing multiple times on a victim to prevent deletion, C2 communication, privilege-escalation techniques, and much more. Due to Hunters International being primarily motivated by financial gain, it is unlikely that the attacks are state-affiliated, and victims were likely targeted due to ease of access. After installing the RAT, due to Hunters International being a Ransomware-as-a-Service (RaaS) provider, it is likely the final payload would be their custom Hunters International ransomware.[xi]
Novel CMoon Worm Makes Gas Industry Squirm	Kaspersky Lab recently detected a new worm dubbed "CMoon" due to strings within its associated files.	CMoon was first seen in July targeting an undisclosed Russian company who supplies the country with "gasification and gas supply," While it could be Gazprom, identification is not certain. The attack was determined to be targeted due to it only affecting visitors of the gas company website, with the attackers replacing legitimate files hosted on the site with their own malicious payload. CMoon itself is written in .NET and has a surplus of built-in tools to accomplish its goals of data theft and remote code execution. Some of its capabilities include antivirus detection, USB device detection, downloading and executing further malicious files, screenshotting, DDoS capabilities, data collection and exfiltration, and more. The worm searches for data worth extracting through various benign applications, such as browsers, SSH/FTP/VPN clients, authentications, messaging software, and more. It also looks for strings such as "secret," "service," and "password" within files, along with checking files with extensions that are likely to hold sensitive data.[xii]
Uncommon Method of C2 Communication in Novel Backdoor	Symantec's threat hunting team released a detailed report regarding a new backdoor that was observed targeting a Taiwanese university.	The backdoor, with the name of "Msupedge," masquerades as a DLL file and utilizes DNS tunneling for C2 communication, using dnscat2 to do so, while leveraging name resolution to send remote commands. Some of the commands it can run allow for process creation, file download, file deletion, and sleep. It is currently unknown the exact way Msupedge was delivered and executed on the Taiwanese campus network. The intrusion is believed to be through an exploitation of a PHP vulnerability known as CVE-2024-4577, which allows for remote code execution on PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, and 8.3.* before 8.3.8, if running in a Windows environment. From their investigations, Symantec has found no evidence attributing this attack to an actor and is currently unsure of the attacker's motivations.
Crossing the River Styx	Check Point Research (CPR) identified a new malware they have dubbed "Styx Stealer," a new information stealer that	Unlike Phemedrone, Styx is not free and is sold via a subscription model. While Styx lacks certain features included in Phemedrone, such as using Telegram for command and control (C2) and encryption capabilities,

	CPR believes to be based off another infostealer, "Phemedrone Stealer."	Styx has added some new abilities such as running automatically, clipboard monitoring, sandbox evasion, anti-analysis techniques, and more. Features present in both stealers include being able to steal browser cookies, passwords, auto-fill data, browser extension data, and saved credit cards from Chromium-based and Gecko-based browsers. Styx can also search and exfiltrate files, obtain location data, gather system information, hijack Discord, Steam and Telegram sessions, check for Wireshark and other debugger activity, and prevent operation in any CIS countries, pointing to a possible Russian connection, be it state-sponsored or cybercriminal in nature. So far, Styx has been seen targeting manufacturing organizations in China, India, UAE, and Philippines.[xiii]
PG_MEM is Anything but Family Friendly	Thanks to Aqua Nautilus researchers, DeepSeas has identified new information about "PG_MEM", a new malware family that is used to target PostgreSQL databases.	PostgreSQL, also known as Postgres, is a free, open-source relational database management system and is one of the most used database management systems (DBMS) in the world. PG_MEM operates by first having the attackers brute force into a PostgreSQL database. Following this, a new local administrator role is created in the breached PostgreSQL environment with elevated permissions. With this account, the attacker will establish persistence, perform discovery about the database, and finally deliver the PG_MEM payload. PG_MEM contains a crypto miner to install on the database, which is the goal of the malware. The crypto miner is intended to silently run on the compromised server, allowing for free use of the victim's hardware to farm cryptocurrency.[xiv]
New Stealer with Mysterious Origins	Cyble Research and Intelligence Lab (CRIL) published their findings about a new information stealer they named "Cheana Stealer", based on the C2 server's name being "ganache[.]live" and the frequent use of the string "ganache" in Cheana's code.	The stealer currently has three variants, targeting Windows, Linux, and macOS. Each of these versions sports similar features, including stealing browser or cryptocurrency wallet information. But they differ in many ways, such as the Linux variant capturing SSH keys, and the macOS version being able to access Keychain. Cyble managed to track Cheana Stealer to a popular Telegram channel with over 54,000 subscribers, where evidence was found to potentially tie this malware back to the Russia state or Russian cybercriminals, as original posts in this channel appear to have been written by a native Russian speaker. However, many communications have come from Arabic speakers as well within the Telegram channel, so ultimate attribution of the author is currently undetermined.[xv]
PEAKLIGHT Puts Up a Fight	Mandiant Managed Defense picked up a sample of a new strain of downloader, which they are internally tracking as "PEAKLIGHT".	PEAKLIGHT is a PowerShell-based downloader that is first delivered through a malicious ZIP archive pretending to hold a copy of a pirated movie. Included in this bundle of files is a LNK file disguised as a downloaded video. Upon execution, the LNK file will reach out to a content delivery network (CDN) operated by the attackers that host an obfuscated JavaScript dropper that runs in memory only. This unnamed JS dropper then executes PEAKLIGHT, which is used to reach out to the attacker's C2 servers to download additional malware. PEAKLIGHT's capabilities include the ability to write to files, run files, download from obfuscated URLs, de-obfuscate strings, and extract data and files from ZIP archives. Additional malware Mandiant saw downloaded

		include the Cryptbot information stealer, SHADOWLADDER malware, and the LUMMAC.V2 infostealer.[xvi]
The Call of Cthulhu Stealer	Cado Security has identified a new malware dubbed “Cthulhu Stealer,” which is a new information stealer written in Golang that specifically targets macOS devices.	Once victims execute the malware posing as an installer for legitimate software, such as “CleanMyMac” or “Grand Theft Auto IV,” they are prompted to enter their device password. The victim’s keychain passwords are stolen as well. Cthulhu then bundles up all the collected data into a ZIP file, which is sent to the attacker’s C2 server. Cthulhu Stealer has the ability to steal cookies, cryptocurrency wallets, Telegram account information, keychain passwords, SafeStorage passwords, and more. The group behind Cthulhu has been named the “Cthulhu Team” and are known to sell Cthulhu Stealer on a monthly subscription basis, with the sale of the malware first seen near the end of 2023. Cado also believes there may be a tie-in between the creators of Cthulhu Stealer and “Atomic Stealer.” Cado stated, “the developer of Cthulhu Stealer probably took Atomic Stealer and modified the code.”[xvii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
APT28 Clears Out Their Garage	Unit 42 has identified a new campaign by the Russian threat actor APT28, an old tactic of using fake, online luxury car advertisements to target foreign diplomats, claiming they have a "Diplomatic Car for Sale." After clicking the ad, the victim is sent to a malicious HTML page, where automation is used to confirm the victim is running Windows and to download the Windows-based “HeadLace” backdoor, which is a multi-faceted backdoor, including a dropper and VBScript launcher. Attribution to APT28 was made by Unit 42 due to the tactics, techniques, and procedures (TTPs) are similar to APT28’s activity in the past. It should also be noted that similar campaigns have been done by other Russian threat groups in the past, such as when APT29 pushed out similar fake car ads (in that instance, BMW-themed lures) to infect devices with lesser malware than HeadLace, further strengthening the connection between this activity and APT28.[xviii]
New APT Group Actor240524 Spreads New Trojans	NSFOCUS Security Labs released new information regarding a novel APT group, which NSFOCUS has marked as “Actor240524.” This group was first seen in July conducting spear phishing against Azerbaijani and Israeli diplomats, intending to steal sensitive data through new weapons. Due to these motivations, it is likely that the group is state affiliated with an opponent of these two countries, however the group’s country of origin is still unknown. The phish sent had a fake but official looking Microsoft Word document attachment containing malicious macros. After enabling macro content, the VBA code is executed, executing the first original malicious trojan made by Actor240524, “ABCloader,” which is used to determine what environment the malware is running. Later a trojan made by the group and named, “ABCsync,” is loaded, which has C2 capabilities, remote command execution, data modification, theft capabilities, and more.[xix]
DeathGrip’s New Hold on the RaaS Market	Researchers at SentinelOne have helped clarify the activity done recently by the newly developed DeathGrip ransomware group. First detected in June, DeathGrip, also known as “Team RansomVerse,” solely operates through Telegram and does not have a data leak site. Despite this covert way of operating, DeathGrip boasts publicly about their ransomware’s capabilities, such as AES256 file encryption, UAC bypass, anti-emulation/bugger detection, artifact deletion, and more. DeathGrip’s ransomware seems to have taken heavy inspiration from LockBit 3.0 and Chaos/Yashma ransomware, with there being different variants of DeathGrip ransomware for both. For the most part, besides slight changes, such as a new ransom note, DeathGrip ransomware is also identical to its predecessors, showing that the group prefers easy, cheap malware rather than developing their own. The ransomware has been seen being distributed through RAR files, which contain a dropper component which retrieves the ransomware payload from the attacker’s remote server.[xx]
PureHVNC Results in Pure Chaos	FortiGuard Labs has published a new article regarding a phishing campaign involving several different malware families, including a newly discovered one that goes by “PureHVNC.” Casting a wide net, the phishes target low-level employees by posing as a customer requesting something, such as a refund, and does not target any particular industry. After opening the attached HTML file, a LNK file is queried causing a malicious BAT file to execute. This BAT not only continues the attack flow, but also deploys a decoy PDF to deter investigation and sets itself to be open upon startup automatically. Continuing the attack, the BAT file downloads two ZIP files containing multiple malicious Python programs, which are obfuscated by a program dubbed “Kramer.” These Python programs then lead to the installation of malware such as XWorm, VenomRAT, and AsyncRAT, along with the aforementioned PureHVNC. PureHVNC, however, is installed differently, using

	Donut as a shellcode generator and “laZzzy” as a shellcode loader. Some functionalities of PureHVNC include C2 communication, information gathering techniques, and more. Based on data collected, the C2 server then installs malicious plugins that further the attacker’s goals. The campaign targets cryptocurrency wallets, password managers, and 2FA authenticators.[xxi]
APT35 Unleashes New Giant, Cyclops	A new malware platform was discovered recently by HarfangLab dubbed “Cyclops,” which may have ties to APT35 (aka CHARMING KITTEN). This platform, written in the Go programming language, offers services such as C2 communication, persistence capabilities, remote code execution, file system enumeration, lateral movement, and more, which is similar to most post-exploitation frameworks. Unfortunately, due to the sample found on VirusTotal, crucial information on how this malware is delivered is not available. Based on previous activity from APT35 regarding their “BellaCiao” malware family, HarfangLab believes that Cyclops is likely to be similarly deployed on Microsoft Exchange Web servers, exploiting vulnerable services. Further connections with Cyclops and APT35 are evident by reuse of multiple domains and IP addresses associated with the group’s previous activity, along with other similar TTPs, such as using similar filenames, relying on SSH tunneling, and using identical usernames and passwords for tunneling.[xxii]
APT42 Shifts Phishing Focus to Israel and the United States	Google’s Threat Analysis Group (TAG) have shared new information regarding APT42, a group operating at the behest of the Islamic Revolutionary Guard Corps (IRGC). Starting around February of this year, the group has been seen shifting around 60% of their total phishing attacks toward sectors such as defense, politics, and academia, along with additional organizations in Israel, and the United States. APT42 often hosts malware and malicious redirects on their phishing sites and are known to abuse cloud storage options such as Google Drive, Dropbox, OneDrive, and others. Some important aspects of the phishes seen sent by APT42 that can be used to identify activity from the group include their malicious use of Google sites, using PDFs with malevolent embedded URLs, along with impersonation and typosquatting techniques. It should also be noted that APT42 is known to use custom phishing kits, such as their G, L, and YCollection credential harvesting tools and DWP, a browser-in-the-browser phishing kit.[xxiii]

Dark Web Markets

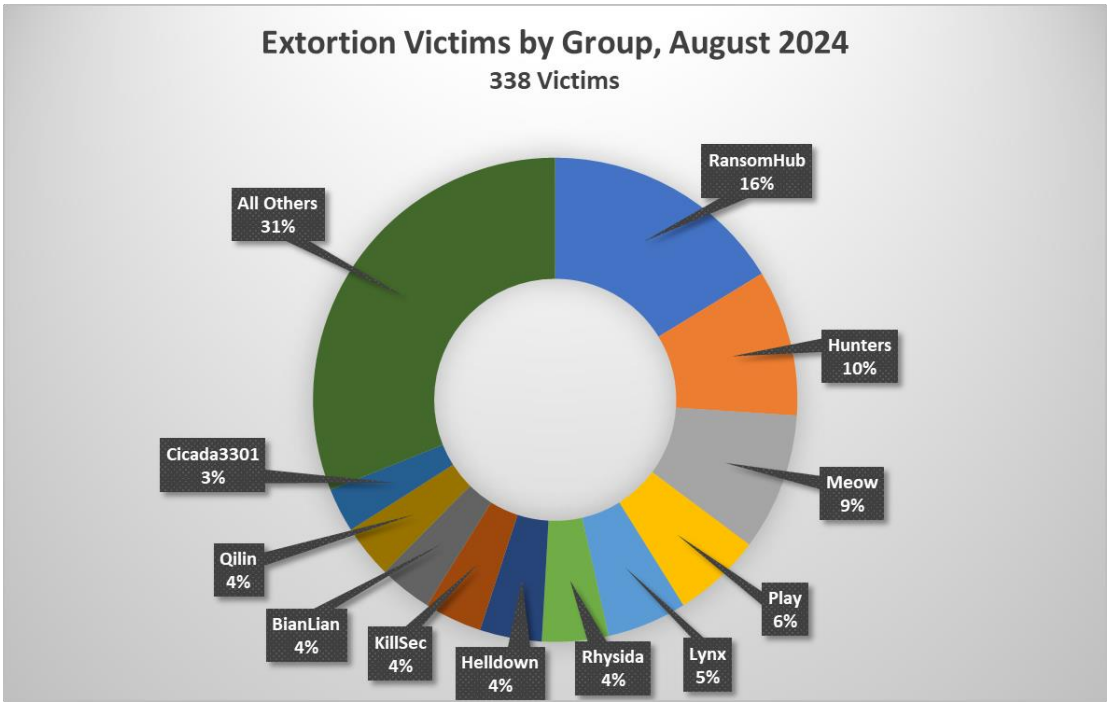
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

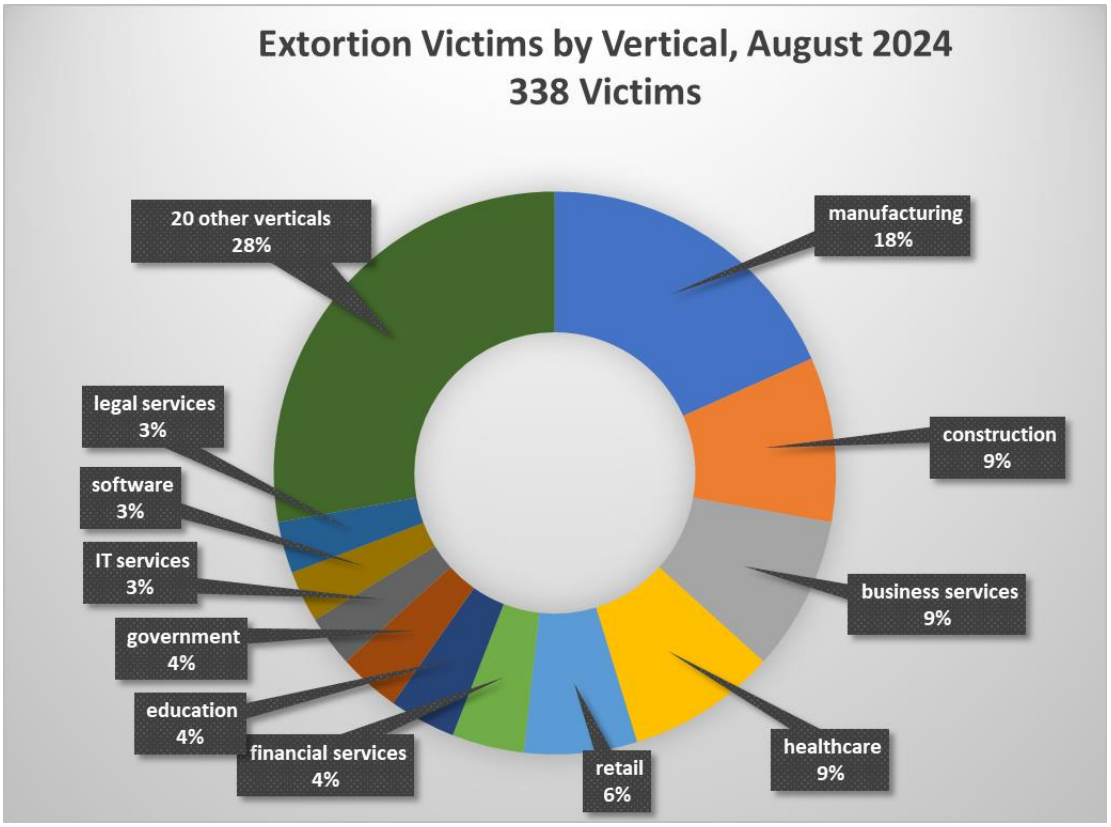
Activity	Note
Data Sale	An actor was observed selling a 415 GB database consisting of 5.8 billion lines of data with URL, username, and password for USD 250. The data was compiled over 2023 and 2024 from public and private sources.
Tool Sale	An actor was observed selling the source code for the Trik/Phorpiex botnet and all modules for USD 6,500. Phorpiex last changed hands in August 2021 for USD 2,500.
Access Sale	An actor was observed selling local user access to a Chilean bank with USD 413.7 million in revenue for USD 2,000.
Access Sale	An actor was observed selling Pulse Secure VPN access to a Taiwanese electronics manufacturer with around USD 20 billion in revenue.
Access Sale	An actor was observed selling RDWeb domain user access to a U.S. based business services company with USD 234 million in revenue and 940 employees.
Access Sale	An actor was observed selling domain admin access to a Filipino company with around USD 7 billion in revenue.
Access Sale	An actor was observed selling RDP access to a US based pharmaceutical manufacturer with more than USD 590 million in revenue.
Access Sale	An actor was observed selling access to an unnamed “big car rental company” with full access to the network and customer PII including driver’s licenses and passports. They did not name a price.
Access Sale	An actor was observed selling multiple avenues of access to "one of the world’s biggest casino software + game providers, if used correctly you could technically trigger jackpots around the world" for USD 80,000. They claimed the victim had USD 3 billion in revenue.
Actor Developments	A notorious criminal forum member claimed to have breached a well-known jewelry retailer. They uploaded a sample of data consisting of data exfiltrated from AWS S3 servers, source code, and other assorted files.
Access Sale	An actor was observed selling full network admin access to what he described as one of the world’s largest manufacturers of construction equipment with USD 67 billion in revenue for a buy now price of USD 150,000.
Actor Developments	The U.S. Department of Justice announced it disrupted two different Russian language cyber crime organizations in the past week. First, the DOJ arrested two Russian asylum seekers in Florida and charged them with various cyber crimes, including being administrators of one of the biggest and most notorious Russian language cyber crime forums, WWH-Club. The forum continues to operate normally, but the community is shaken. Second, the DOJ announced the shutdown of the Radar AKA Dispossessor ransomware operation. The operation used Digital Ocean and other western hosting services. While the servers were seized and the operation disrupted, no arrests were made, and one of the suspected members even remains an active member of several Russian language cybercrime forums.
Access Sale	An access seller was seen to be selling VPN RDP domain user access to a U.S. based aerospace and defense company with USD 3.2 billion in revenue for USD 3,000.
Access Sale	An access seller was observed selling VPN domain user access to the domain controllers belonging to an Indonesia based enterprise in the airlines, airports, and air services vertical with USD 456.8 million in revenue for USD 800.

Access Sale	An access seller was noted to be selling Cisco VPN domain user access to a U.S. based test and measurement equipment manufacturing enterprise with USD 1.5 billion in revenue. The seller is likely in a partnership with the former proprietor of Radar/Dispossessor ransomware, whose infrastructure was dismantled by law enforcement last week.
Access Sale	An access seller was seen selling access to what he claimed was a major distributor of propane gas in the United States. They did not name a price.
Access Sale	An access seller was observed selling RDweb domain admin access to a Canadian enterprise in the marine shipping and transportation vertical with more than USD 550 million in revenue.
Access Sale	An access seller was observed selling VPN access to a company in the cable and satellite vertical with USD 19.2 million in revenue for USD 1,000. In describing the victim, the actor used verbiage copied directly from the victim's website.
Access Sale	An actor was seen selling MySQL server access with "all privilege" to a US based company with more than USD 16 billion in revenue and a market capitalization of more than USD 4 billion for USD 27,000. The actor just joined the forum on 21 August and his track record is unknown.
Data Sale	A reputable actor was observed selling a "fresh" database with information on 1.2 million customers of a major casino in the US and Canada. The price is USD 1,000 per 120,000 lines.

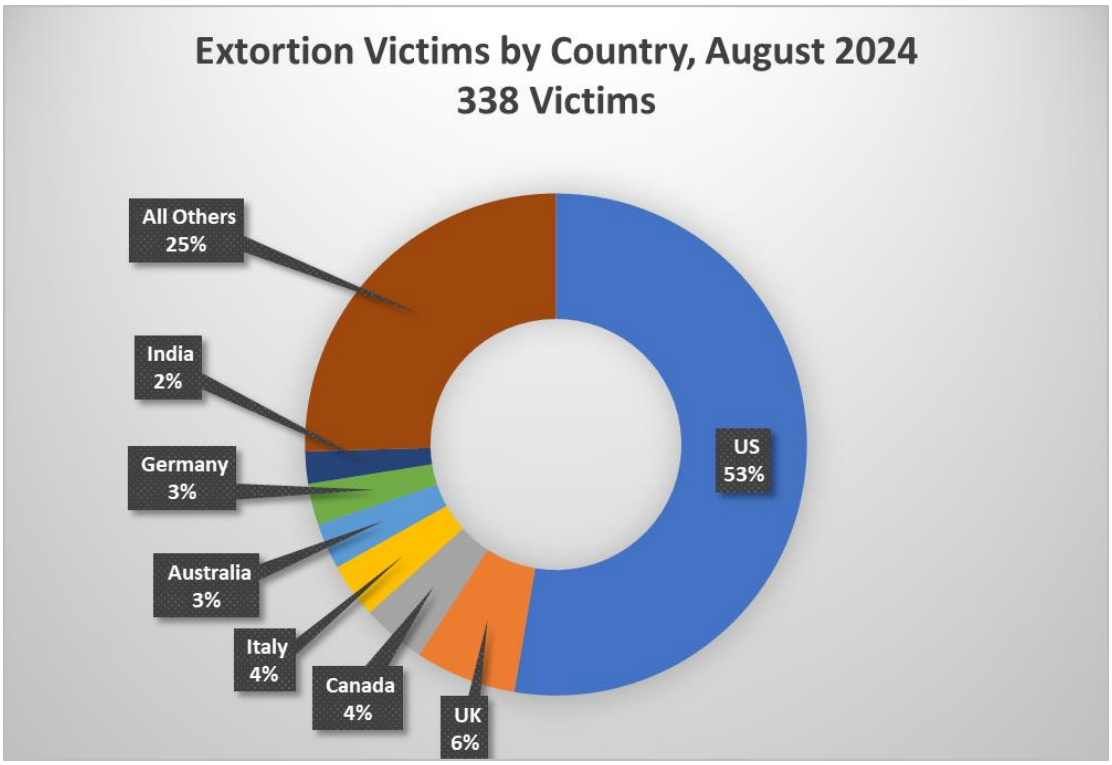
By The Numbers

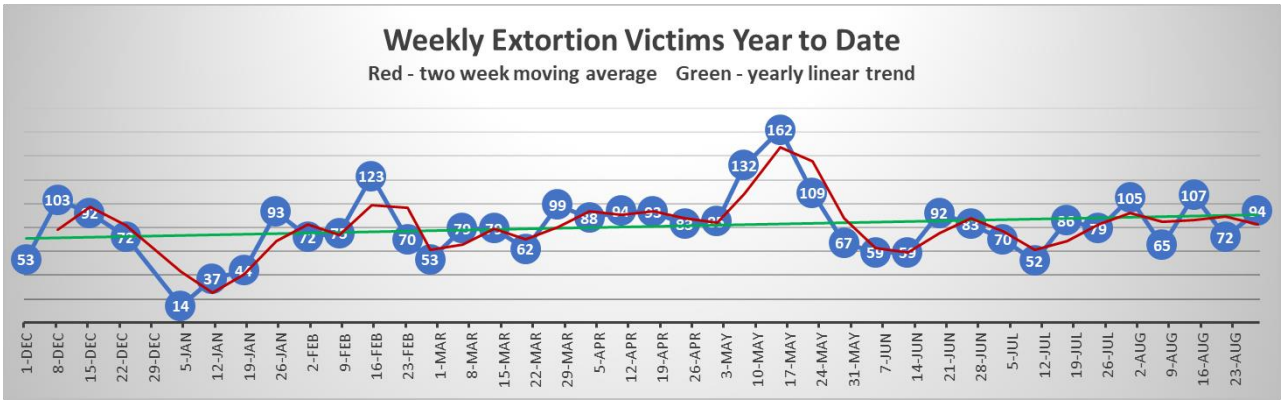
Summarizing incidents in graphical format

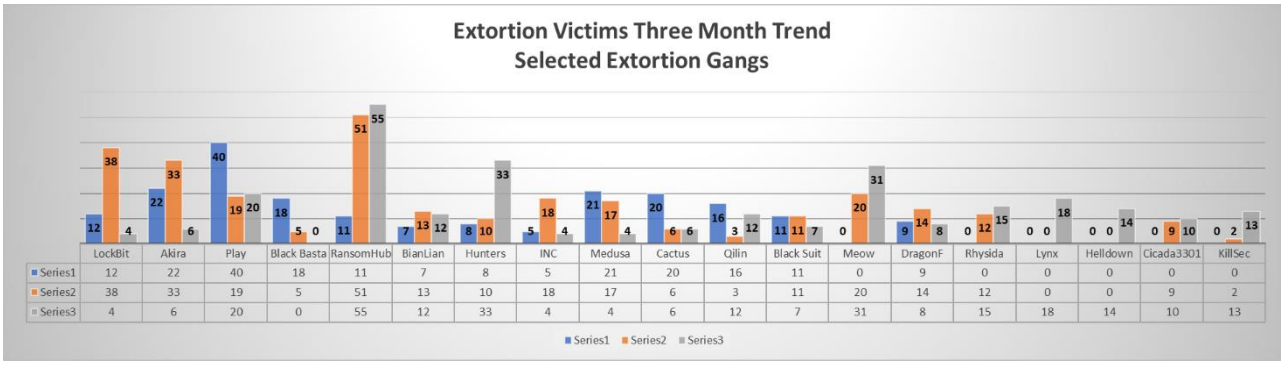




TLP:CLEAR


Extortion Victims by Country, August 2024
338 Victims
All Others 25%
India 2%
Germany 3%
Australia 3%
Italy 4%
Canada 4%
UK 6%
US 53%


Weekly Extortion Victims Year to Date
Red - two week moving average Green - yearly linear trend
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


Extortion Victims Three Month Trend
Selected Extortion Gangs
LockBit Akira Play Black Basta RansomHub BianLian Hunters INC Medusa Cactus Qilin Black Suit Meow DragonF Rhysida Lynx Helldown Cicada3301 KillSec
Series1 12 22 40 18 11 7 8 5 21 20 16 11 0 9 0 0 0 0 0
Series2 38 33 19 5 51 13 10 18 17 6 3 11 20 14 12 0 0 9 2
Series3 4 6 20 0 55 12 33 4 4 6 12 7 31 8 15 18 14 10 13
Series1 Series2 Series3

TLP:CLEAR

New Detection Content

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

- Defense Evasion - AMSI - Executable File (PE) Discovered In-Memory – Modified
  - An attacker can evade anti-malware technologies by embedding encoded content within a script and then loading that into the memory of the running process. Signature is from CB AMSI Threat Intelligence.
- Google Cloud SCC: Malicious Binary or Script Executed
  - The analytic looks for a binary, script, or library being executed that was identified as malicious based on threat intelligence. The findings associated with this activity include Added Malicious Binary Executed, Added Malicious Library Loaded, Built in Malicious Binary Executed, Modified Malicious Binary Executed, Modified Malicious Library Loaded, and Malicious Script Executed.
- Google Cloud SCC: Credential Access
  - This analytic alerts on Google Cloud Security Command Center credential access detections. Examples of this activity include external members being added to privileged groups, privileged groups being opened to the public, secrets accessed in Kubernetes namespace, and sensitive roles being granted to hybrid groups.
- Google Cloud SCC: Malware Findings
  - This analytic alerts on Google Cloud Security Command Center malware detections. Examples of this activity includes detection of exploit traffic, malware, or crypto miners based on connections to, or a lookup of, known bad domains or IP addresses.

[i] https://reasonlabs.com/research/new-widespread-extension-trojan-malware-campaign
[ii] https://cyberint.com/blog/research/meet-uuloader-an-emerging-and-evasive-malicious-installer/
[iii] https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/
[iv] https://www.elastic.co/security-labs/beyond-the-wail
[v] https://www.cloudsek.com/blog/major-payment-disruption-ransomware-strikes-indian-banking-infrastructure
[vi] https://correctiv.org/faktencheck/russische-desinformation/2024/08/13/doppelgaenger-kampagne-russland-nach-correctiv-veroeffentlichung-bricht-bei-russischen-propaganda-machern-hektik-aus/
[vii] https://www.esentire.com/blog/a-dropper-for-deploying-gh0st-rat
[viii] https://www.elastic.co/security-labs/bits-and-bytes-analyzing-bitsloth
[ix] https://any.run/cybersecurity-blog/deerstealer-campaign-analysis/#stealer-8460
[x] https://blog.sonicwall.com/en-us/2024/08/sonicwall-discovers-second-critical-apache-ofbiz-zero-day-vulnerability/
[xi] https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/
[xii] https://securelist.ru/how-the-cmoon-worm-collects-data/109988/
[xiii] https://research.checkpoint.com/2024/unmasking-styx-stealer-how-a-hackers-slip-led-to-an-intelligence-treasure-trove
[xiv] https://www.aquasec.com/blog/pg_mem-a-malware-hidden-in-the-postgres-processes/
[xv] https://cyble.com/blog/new-cheana-stealer-targets-vpn-user/
[xvi] https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware
[xvii] https://www.cadosecurity.com/blog/from-the-depths-analyzing-the-cthulhu-stealer-malware-for-macos
[xviii] https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/
[xix] https://nsfocusglobal.com/new-apt-group-actor240524-a-closer-look-at-its-cyber-tactics-against-azerbaijan-and-israel
[xx] https://www.sentinelone.com/blog/deathgrip-raas-small-time-threat-actors-aim-high-with-lockbit-yashma-builders/
[xxi] https://www.fortinet.com/blog/threat-research/purehvnc-deployed-via-python-multi-stage-loader
[xxii] https://harfanglab.io/insidethelab/cyclops-replacement-bellaciao/
[xxiii] https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/