Monthly Threat Intelligence Rollup

DEEP seas

07/01/24-07/31/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
CRYSTALRAY's Bright Debut	The Sysdig Threat Research Team has increased their attention this week on a new threat group which Sysdig has dubbed "CRYSTALRAY." CRYSTALRAY first appeared in February, utilizing "SSH-Snake," an open-source worm not written by the group, to leverage compromised SSH credentials to further spread the worm on a network. Their motivations appear to be financial, with the goal of collecting and selling credentials and deploying cryptominers. The group has expanded since February to allegedly ten times its previous size, targeting over 1,500 new victims, and has even begun to incorporate more capabilities into their toolkits, such as adding other open-source tools like zmap, asn, httpx, nuclei, Platypus, and Sliver. Although they do not write much code in-house, some custom code written by CRYSTALRAY allows for the removal of other cryptominers that the victims may already be running, eliminating competition for the victim's computing resources.[i]
CrowdStrike Bug "Fixes" Appearing Online	Various independent researchers on X have identified examples of fraudulent CrowdStrike "hotfixes" online. The first was cybersecurity researcher @g0njxa, who helped expose a hidden malicious archive file hosted on a phishing site. This file was used to target Spanish bank Banco Bilbao Vizcaya Argentaria, one of the largest financial institutions in the world. Within this document are instructions stating that the file is used for a "mandatory update to avoid connection and synchronization errors to the company's internal network." Malware sandboxing and analysis service AnyRun also chimed in, stating that the fake update first delivers HijackLoader, following up with Remcos for remote access. In another example, again pointed out by AnyRun, the company noticed another fake CrowdStrike update which was secretly a data wiper. Delivered via phishing, this wiper is downloaded by the victim after clicking on a web link in the attached PDF file.[ii]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
New MerkSpy Leverages Microsoft Office Exploit	A recent report by FortiGuard Labs' threat research team provides details regarding a new piece of spyware they have dubbed "MerkSpy."	Although it is unknown who developed or uses MerkSpy, it is known that the malware was designed for various purposes of possible espionage, including monitoring user activities, stealing sensitive information, establishing persistence, keylogging, screenshotting, and harvesting Chrome browser login data. A MerkSpy infection begins by exploiting a vulnerability in the MSHTML component used by Internet Explorer in Microsoft Office (CVE-2021-40444), allowing for an attacker to execute code after the victim opens the document. After abusing this vulnerability, MerkSpy downloads a file named "olerender.html," which contains JavaScript and other embedded shellcode. This HTML file is then deciphered to execute the injector responsible for loading MerkSpy into memory and integrating it with other active system processes.[iii]
InnoLoader Gets "InYo" Face	ASEC has discovered the distribution of a new malware variant that disguises itself as a software crack or a commercial tool.	The malware, which ASEC has termed "InnoLoader," utilizes a user interface in which malicious actions are only taken after using the UI during installation, rather than performing malicious behaviors immediately upon startup like most malware. It is also worth noting that each time the malware is downloaded, it is freshly created, meaning each victim will have a copy of InnoLoader that has a different hash but the same functions. The loader got its name from being created by InnoSetup, which is a script used to control all aspects of the Windows installation process, including what files should be installed and where, what shortcuts should be made and what they should be named, and more. After successful installation and execution, InnoLoader then reaches out to any of six C2 domains, where any number of malicious info stealers, browser plugins, adware, and more can be further installed on the victim.[iv]
Kematian-Stealer Malware Enters the Scene	On 6 July, research firm Cyfirma released a report containing their analysis of a purportedly new information stealer malware they have dubbed Kematian-Stealer, an open-source malware available on GitHub.	The Kematian-Stealer malware is not particularly novel in the information that it targets: passwords, browser cookies, desktop screenshots, cryptocurrency wallets, and others. Instead, the malware is fully loaded with a suite of evasive features, including executing in-memory, downloading and executing scripts, payloads and modules directly into memory space, as well as hosting the builder on GitHub. This last point is likely to lead to widespread use of Kematian-Stealer by low-level cybercriminals, as features and command and control server information may be configured via a simple web UI. The author's use of GitHub is not likely to last long, as GitHub has a history of quickly taking down or removing such services. This is most likely a form of advertisement utilized by the author to demonstrate that their tool is legitimate and useful. The codicil of "for educational purposes only" is unlikely to provide much defense against legal action against the author(s), though it does seemingly provide a veneer of legitimacy. Kematian-

		Stealer also utilizes Discord for C2 communications, which may provide an easy method of post-compromise detection in the event that the malware is downloaded and executed.[v]
Oh No…Not POCO!	The team at Cofense Email Security has recently discovered a new remote access trojan which has since been named “Poco RAT” by the company.	This was due to malware utilizing the POCO C++ libraries, a popular set of class libraries used for developing the network functionality for C++ applications. The threat actor behind the trojan is currently unknown but has been seen previously targeting Spanish-speaking companies in the mining sector and has since grown to attack the manufacturing, hospitality, and utilities sectors. The delivery of Poco RAT consistently starts with a phishing email, which attempts to infect the user by having them open or click on malicious attachments or links. The RAT itself is an executable that was written in Delphi, with the main goals of establishing persistence, process injection, C2 communication, and the delivery of further malware, such as information stealers or ransomware.[vi]
Killer Ultra is Ultra Scary	ARC Labs has recently identified a tool which is paired with Qilin ransomware to disable popular antivirus and EDR tools, such as those from Symantec, Microsoft, and SentinelOne.	This tool, which ARC Labs has named “Killer Ultra” due to a module having the same name within the malware, leverages vulnerability CVE-2024-1853 within Zemana AntiLogger, an anti-keylogging software for execution. This vulnerability exploits Zemana AntiLogger’s drivers, allowing the attacker to terminate any processes at will, including the aforementioned examples given of antivirus or EDR tools. Some of the capabilities of Killer Ultra include obtaining kernel-level permissions and itemizing and clearing Windows Event Logs, along with inactive code that has the capability to use post-exploitation tools for the purpose of downloading and executing data over a C2 channel. It also sports virtualization and sandbox evasion techniques, detecting files on the victim’s devices that may indicate it is running in a virtual machine, such as VirtualBox or CAPE.[vii]
MuddyWater’s BugSleep Backdoor is Nothing to Sleep On	Check Point Research has exposed recent changes in the Iranian state-aligned MuddyWater group.	As the group continues to bombard various Israeli sectors in its many Israel-directed campaigns, an original, previously undocumented custom backdoor was found and labeled “BugSleep” by CPR (also known as “MuddyRot” by Sekoia). This name was given due to the many calls BugSleep makes to the Sleep API, a library powered by Google Play services that allows apps to determine when the user goes to sleep and wakes up. It does this to flood the victim to hide when BugSleep loads the appropriate APIs it needs to run properly to evade detection. The backdoor is initially sent through phishing emails that have a PDF attachment with a malicious link. This link then downloads a ZIP file which is hosted in Egnyte, a secure file-sharing platform which contains the BugSleep malware. While BugSleep does not differ much from other backdoors primarily being used to execute commands and transfer files between the victim and MuddyWater’s C2 server, it does have some notable features. One of these is a loader for BugSleep, which helps inject BugSleep into the memory space of legitimate processes such as Chrome, AnyDesk, OneDrive, and PowerShell.[viii]
Void Banshee Explores New Vulnerabilities	Trend Micro’s Zero Day Initiative threat hunters have identified a new zero-day vulnerability in one of Microsoft’s end-of-life (EOL) products, the Internet Explorer browser.	CVE-2024-38112 can be used to compromise a victim’s devices and execute malicious files through Internet Explorer using MSHTML. This exploit has been used primarily by Void Banshee, an APT group that is known for targeting North America, Europe, and Southeast Asia with the goals of information theft and financial gain. Void Banshee utilizes the spear phishing victims to gain initial access with an attached

		ZIP file which holds malicious files pretending to be PDF documents. These ostensible PDF documents are actually URL files that can be used to exploit CVE-2024-38112 and trick the user into opening a webpage hosting a malicious HTML application. After the malicious HTML application is clicked, a VBS script is executed, which then launches a PowerShell script to fetch multiple different loaders, including a modified version of Donut Loader. Donut Loader finally installs the Atlantida stealer on the victim's device, accomplishing their ultimate goal.[ix]
APT41's Swiss Army Knife of Malware	Google's Threat Analysis Group has detected new activity from APT41, a well-known Chinese state-sponsored threat group that conducts espionage activity, along with other financially motivated activity that may be outside of state control.	Recently the group has been seen successfully targeting the shipping, media, technology, and automotive sectors in Italy, Spain, Taiwan, Thailand, Turkey, and the United Kingdom. APT41 first infects the victim with both the ANTSWORD and BLUEBEAM web shells to establish a foothold and persistence in their environment. Using these web shells, APT41 further installs the DUSTPAN dropper to download the BEACON backdoor to help establish a C2 connection. After this, the group adds another loader to the victim's device, the DUSTTRAP dropper. This dropper allows for even more malicious tools to be installed, such as SQLULDR2 to copy data from the victim's databases and PINEGROVE to exfiltrate said data back to the attackers.[x]
Play Ransomware Amuses Itself with New Linux Variant	Trend Micro's threat hunting team has identified an update to the Play ransomware, which now has a Linux variant that can target ESXi environments.	The group behind the Play ransomware is known for its considerably large impact on various organizations in Latin America. The chain of infection for this strain of Play ransomware begins with a phish containing a malicious RAR attachment. This RAR attachment reaches out to the group's C2 server, which holds much of their formal tools of the trade, including NetScan for discovery, PsExec for lateral movement, the Coroxy backdoor for C&C, and WinSCP and WinRAR for exfiltration. Using these tools, the threat actor then attempts to execute the Play ransomware on the victim's devices. Interestingly, Trend Micro noticed a connection between the Play ransomware group and Prolific Puma, another group which provides shortened links for threat actors for profit. The groups have shared IPs and domains, hinting that Prolific Puma may be offering the Play Ransomware group its services.[xi]
Daggerfly Invests in a New Toolset	Symantec's threat hunting team has released a report regarding updates to the toolset of the threat group Daggerfly.	Daggerfly is a Chinese state-affiliated APT group that has been active since around 2012, conducting cyber espionage with targets varying from individuals to government institutions and organizations. The new tools used by the group include MgBot, Macma, and Suzafk. MgBot is a backdoor framework developed and used exclusively by Daggerfly to steal information and perform espionage. Macma is a macOS backdoor that uses privilege escalation vulnerability CVE-2021-30869 to install itself. Remarkably, through this investigation Symantec was able to determine that Daggerfly was also the creator of Macma due to a shared infrastructure and library with MgBot. The malware's origin was previously unknown. Suzafk is a brand new, Windows-based, multi-staged backdoor by Daggerfly that can use TCP or OneDrive for its C2 functionality.[xii]
XDSpy Unleashes DSDownloader	FACCT threat intelligence specialists published their analytical findings of a new downloader being	This downloader was sent to an undisclosed Russian IT company and possibly entities in Moldova. The downloader is named "DSDownloader" by FACCT, with "D" meaning dropper and "S" meaning sideloading. The malware is distributed

	delivered by the XDSpy cyber espionage group, a very stealthy group known for starting their malicious activities in 2011 and going almost completely undetected until 2020.	through phishing emails that hold a malicious link that downloads a RAR file containing the downloader. Upon execution, the malware first opens a decoy PDF document to distract the victims. Next, it adds itself to the victim's startup programs by manipulating parameters in the victim's Windows Registry. Finally, the malware transfers its final payload from XDSpy's servers and executes. The final payload at the end of this infection chain has yet to be recovered.[xiii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Kimsuky in Good Spirits with HappyDoor Malware	AhnLab Security intelligence Center (ASEC) recently published an analysis of a previously undisclosed backdoor, which ASEC has named “HappyDoor” due to the word “happy” being listed alongside the malware’s version number. This backdoor has been used by the Kimsuky group since 2021, being distributed through attaching the malware to phishing attempts. Due to being a DLL file, HappyDoor works through the regsvr32 utility, where it installs itself and deletes other files, adds a new extension to itself (*.OTP) and duplicates, then performs the various malicious actions it sought out to do. Some of these features include screenshotting, keylogging, collecting data on connected devices, microphone access, data exfiltration, and more.[xiv]
Google Chrome Extension Turned Spyware	Zscaler makes note of a new Google Chrome extension used by Kimsuky while passively monitoring them. This extension, which Zscaler has dubbed “TRANSLATEXT,” appears to operate as spyware, allowing attackers to steal email addresses, usernames, passwords, and cookies and capture browser screenshots. The infection chain begins with a ZIP file that holds an executable. Upon launch, the executable fetches a PowerShell script (hades.txt) that collects and uploads the victim’s data to GitHub, along with creating a Windows shortcut that downloads even more PowerShell scripts which are used to establish a C2 connection. It should also be noted that TRANSLATEXT has also been seen bypassing the built-in security measures of multiple, well-known email providers such as Gmail, Kakao, and Naver. Attribution of this activity to this group is due to the target vector being South Korean academia focused on political research related to North Korea, a target that fits Kimsuky’s modus operandi.[xv]
Japan on the Receiving End of More 'Just Kimsuky Things'	Another North Korean campaign attributed to the Kimsuky group has been reported by JPCERT, this time consisting of phishing lures impersonating security and diplomatic organizations. The lure documents are easily identified by many spaces trailing the false file extension, a curious change of tactic on Pyongyang's part, but one which may prove more successful than suspected at first glance. Multiple components are dropped upon execution of the lure document, including a system profiler component and a VBS-based keylogger component, hinting at a purely espionage-based motivation behind the attacks. The use of the native Windows wscript feature to retrieve a PowerShell script from an attacker-controlled remote resource is not unique to Kimsuky but coupled with the use of a Visual Basic Script (VBS) file to call wscript to do so matches recently observed tactics utilized by the Kimsuky group and points towards the group's involvement. Though this attack targeted South Korean organizations, the group has not restricted their operations purely to the Korean peninsula. Japan, China, Russia, and other ASEAN and foreign nations have been targeted by Kimsuky in the past, and thus caution is warranted.[xvi]
CloudSorcerer Group Targeting Russian Government Entities	In May 2024, Russia-based Kaspersky Lab reported on a new threat group targeting Russian government entities with unique malware that utilizes cloud-based services for command and control (C2) and data exfiltration. Dubbed 'CloudSorcerer,' Kaspersky does not make overt claims of attribution, though the implication is that either Ukraine or other western nations are behind the group's operations. CloudSorcer also has some overlap with other groups that have attacked Russian entities in recent years, including the CloudWizard group, though Kaspersky researchers point out that the group's toolset is completely different from previously seen CloudWizard tools. This may mean that CloudWizard has completely retooled their arsenal or another group, entity, company, government, etc. has stepped in with a new toolset. The group's malware has only been observed being delivered on machines which were previously compromised; details of these compromises were not provided, unfortunately. The malware is a fully featured

	backdoor written in C which makes use of Microsoft's COM object interfaces for operations and can operate in at least two distinct modes (backdoor and C2 relay) from a single executable. This is efficient for day-to-day operations, but the attackers run the risk of losing their access to a compromised endpoint entirely via this method. The 'Cloud' appellation stems from the malware's use of cloud-based services for C2 and exfiltration. Yandex, Mail.RU, Microsoft Graph, and Dropbox have all been observed being abused by the CloudSorcerer's flagship backdoor.[xvii]
APT41 Activates New Arsenal: DodgeBox and MoonWalk	The Zscaler security research team has uncovered two novel pieces of malware attributed to the Chinese nation state threat actor APT41. This malware toolset includes “MoonWalk,” a backdoor, and “DodgeBox,” a loader that is used to download the MoonWalk backdoor to victim’s devices. Interestingly, both seem to share a common development toolkit. In addition, DodgeBox appears to be a variant of “StealthVector,” another known loader used by APT41. Altogether this points to APT41 as the likely developers of these malicious tools. As for the malware itself, DodgeBox can employ a variety of detection evasion techniques along with the usual loader duties, such as call stack spoofing, DLL sideloading, DLL hollowing, and environmental guardrails. MoonWalk’s capabilities as a backdoor include information gathering, token impersonation, command execution, and more. Additionally, it uses similar evasive techniques to DodgeBox, along with C2 communication using Google Drive. For antivirus and EDR evasion, Windows Fibers was used, which is a form of user-mode scheduling by Microsoft that allows applications to manage their own threads of execution.[xviii]
Kimsuky Trolls South Korea with Novel TrollAgent	Thanks to research done by the Dark Atlas Squad, we now have new intelligence on Kimsuky’s latest project, “TrollAgent.” TrollAgent is an information stealer that is delivered through a malicious executable which drops the stealer in the form of a DLL file written in GoLang. The executable also drops a batch file to remove the initial installer upon dropping the DLL. The stealer is protected using VMProtect3, a software protection tool which is used to protect applications from reverse engineering, cracking, or any unauthorized tampering. Due to this, reverse engineering is difficult due to VMProtect3’s anti-debugging techniques and code virtualization. TrollAgent can harvest a wide range of browsers’ data like other stealers; in fact, it has a dedicated handling function for each browser such as Chromium or Firefox. It also has the functionality to collect credit card information, cookies, browsing history, and auto-login credentials from these browsers.[xix]
APT28 Strikes Again at Ukraine with HATVIBE and CHERRYSPY	Various researchers have linked a new cyber espionage campaign against Ukraine's scientific and research institutions to the Russia-backed group APT28, also known as Fancy Bear or BlueDelta. The group used the malware strains known as HATVIBE and CHERRYSPY during attacks in July 2024. HATVIBE allows for file downloads and execution on infected devices, while CHERRYSPY enables remote Python code execution. These tools were previously deployed by APT28 in a May 2024 campaign against a Ukrainian government agency. In this latest attack against Ukraine, however, hackers accessed an employee's email account to distribute a malicious document. CERT-UA, the Computer Emergency Response Team of Ukraine, was able to record numerous HATVIBE installations by noticing that APT28 had exploited a vulnerability in HFS, which is a web server application intended to allow sharing and transferring files over HTTP. The espionage group has been in operation for well over a decade, with targets extending beyond Ukraine to include Mongolia, Kazakhstan, Kyrgyzstan, Israel, India, Armenia, Germany, Poland, and the Czech Republic, as well as numerous NATO nations abroad.[xx]
A New APT Group Joins the Ranks: APT45	The Mandiant threat intelligence team has officially named a new APT group: APT45. This group has a long history despite only recently being classified. Starting back in 2009, APT45’s first duties solely involved running espionage campaigns for North Korea, however, the group has since grown to also commit cyber crime for financial gain, likely to support the group’s members and the North Korean government as a whole. Sectors APT45 is known to target include government entities, defense, finance, nuclear power, agriculture, healthcare, and pharmaceuticals, to name a few. The threat

	group also uses a plethora of malware for their goals, ranging from publicly available tools, modified publicly available malware, and even their own custom malware families. Overlap with other North Korean threat groups has also been identified, with Mandiant stating with a high degree of confidence that APT45 has strong connections to groups such as Andariel and Lazarus.[xxi]

Dark Web Markets

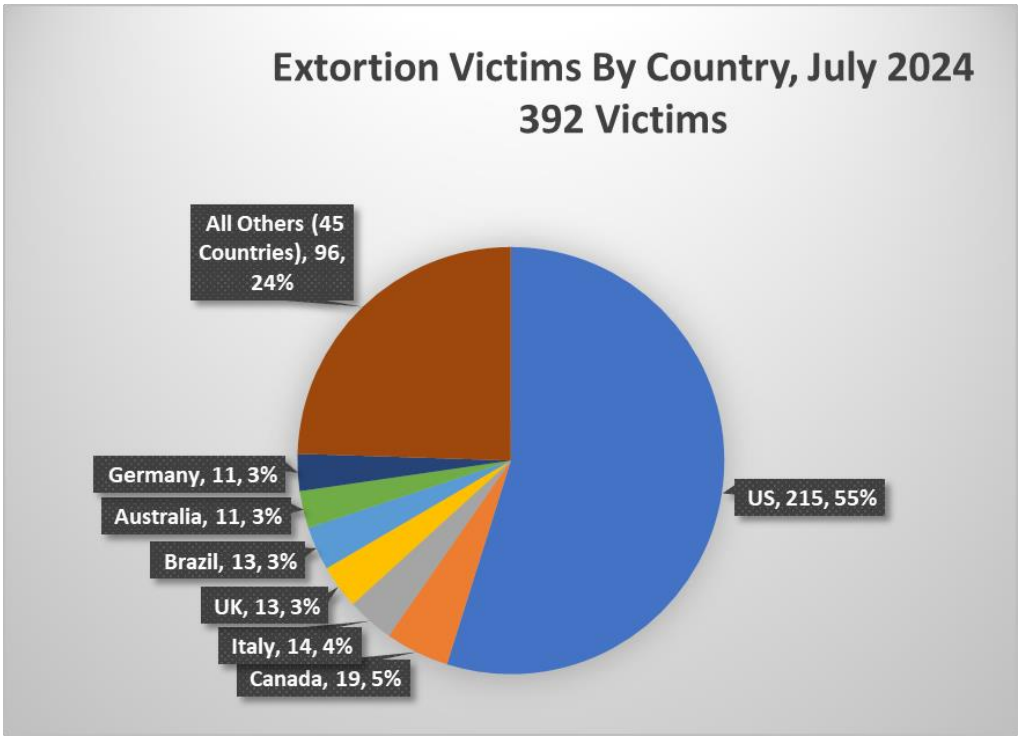
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

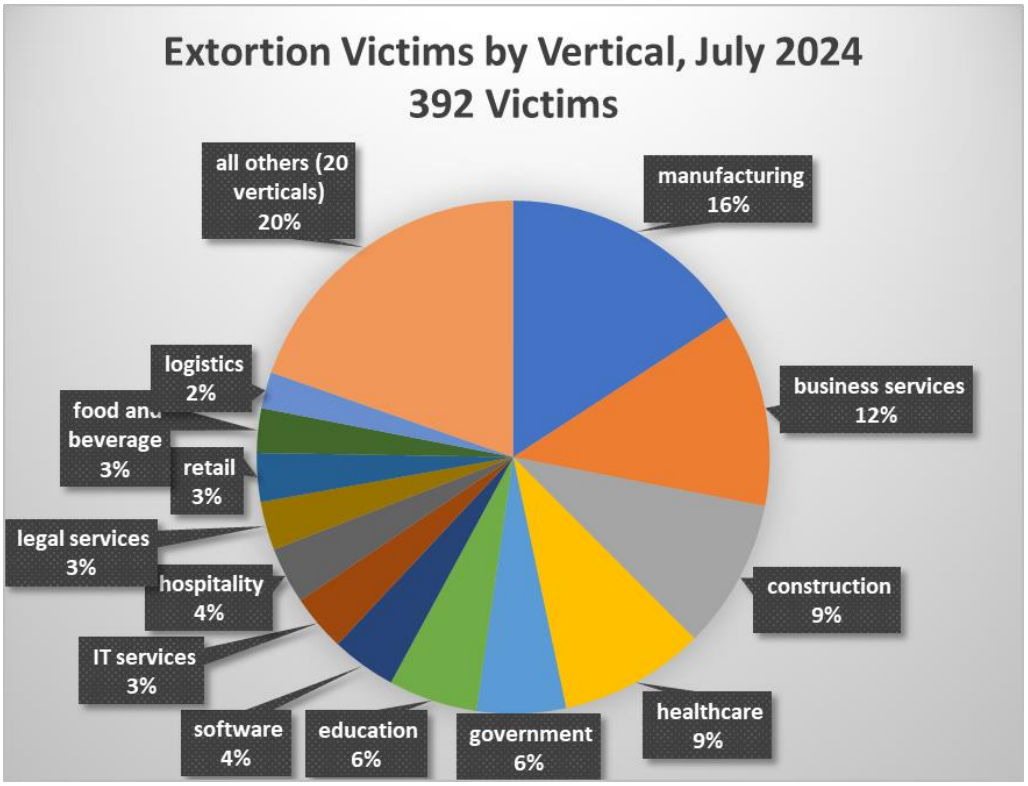
Activity	Note
Access Sale	An actor on a Russian-language crime forum was selling Apache Solr access to a U.S.-based credit report company with less than USD 4 billion in revenue.
Access Sale	An actor on a Russian-language crime forum was selling Fortinet VPN domain user access to a large Thai manufacturer with USD 17 billion in revenue for USD 5,000.
Access Sale	A new actor on a Russian-language crime forum was selling accesses to two hospitals in Tennessee and New Hampshire.
Access Sale	A new access seller on a popular crime forum was selling access to two U.S.-based oil and gas enterprises, one with more than USD 55 billion in revenue for USD 3,000 and a second unnamed enterprise with more than USD 5 billion in revenue for USD 2,000.
Access Sale	An actor was observed selling access to an unnamed “gas manufacturer” described as “the largest in its industry in the U.S. region” with USD 4 billion in revenue for USD 4,000.
Access Sale	An actor on a Russian-language crime forum was selling access to a large education institution for USD 1,500.
Actor Developments	An actor was observed posting documents supposedly stolen from a prominent defense contractor. The documents included proprietary information concerning rate charging and business processes and several government documents marked “Exempt from FOIA” with employee counterintelligence reports of suspicious foreign contacts.
Access Sale	A new English-speaking actor was observed selling SMTP logins and databases belonging to what was eventually revealed to be a major U.S. port. They claimed to have access to emails, password hashes, and an AWS key for a subdomain belonging to the port. They also posted screenshots purporting to prove their access.
Actor Developments	A new actor released 1.1 TB of Slack records belonging to a major U.S. entertainment company, purporting to cover every message in 10,000 channels.
Actor Developments	Russian authorities responded to a German demand for the arrest of Fedor Aleksandrovich Andreev, a suspected member of the group responsible for TrickBot. It is likely that Russia responded to the request in order to maintain access to the Interpol red notice system, which Russia uses to track down and arrest dissidents in exile. Although they complied with the arrest warrant, Andreev is unlikely to be extradited as extradition of Russian citizens to foreign countries is prohibited under the Russian constitution.
Data Sale	An actor on an English-language crime forum was selling what they claimed is source code belonging to a major U.S. publication. Based on a Pastebin link provided by the actor, it appears that they may have gained access to the publication’s Git repository.
Data Sale	An actor was observed giving away 9.5 GB of data belonging to a Texas-based oil field services company. Supposedly, this company is a partner of half a dozen oil and gas companies. Their explicit goal was to "see Colonial Pipeline 2.0 or Stuxnet 2.0."
Data Sale	A notorious actor claimed to have scraped 250 million IOCs used by CrowdStrike directly by systematically abusing CrowdStrike endpoints over the period of a month. The data is proprietary but provided to customers. Two of the customers whose endpoints they abused were an unnamed oil company and a non-U.S. pharmaceutical company.

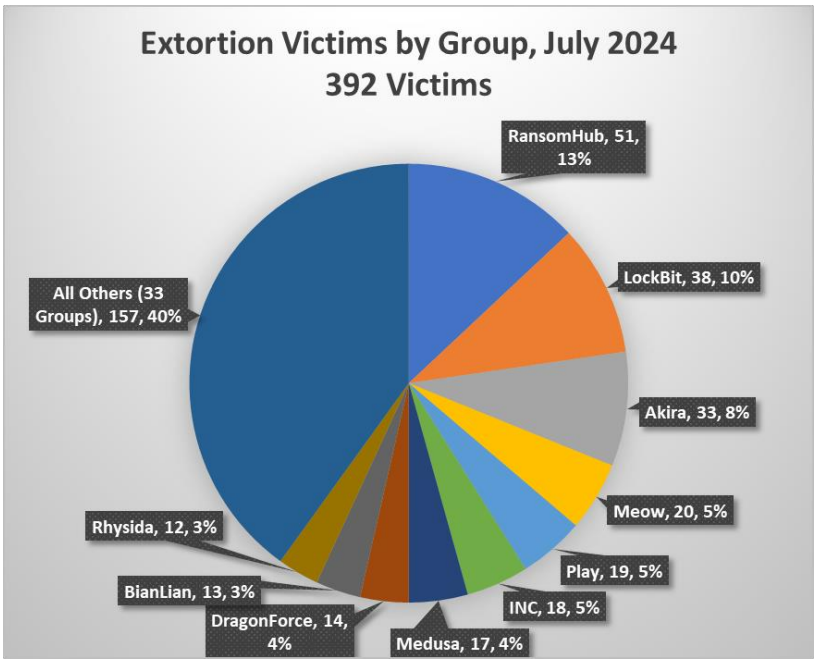
Access Sale	An actor was observed selling RDP access to an unnamed U.S. auto parts store with more than USD 250 million in revenue for USD 1,800.
Data Sale	A notorious actor on multiple crime forums was observed selling more than 3 TB of prescription drug data stolen from a medical company, likely through a known vulnerability in Snowflake that has recently been exploited by actors. They claimed that the data would allow a purchaser to write their own drug prescriptions. The actor is extorting the healthcare company in question for USD 3 million dollars, or they are willing to sell the information for USD 1,000 per line of information with a discount for bulk purchases.
Access Sale	An actor was observed selling AnyDesk access to a U.S.-based media and internet company with USD 51.5 million in revenue for USD 3,500.
Access Sale	An actor was observed selling access to “the core server room” of a “U.S. world famous IT giant” for USD 50,000. They originally stated that the company had USD 30 billion in revenue and later adjusted it to more than USD 50 billion. The actor was subsequently banned from the forum for attempting to sell access to one of the largest Russian companies. Attacks against entities in the former Soviet Union is strictly prohibited in most crime forums.

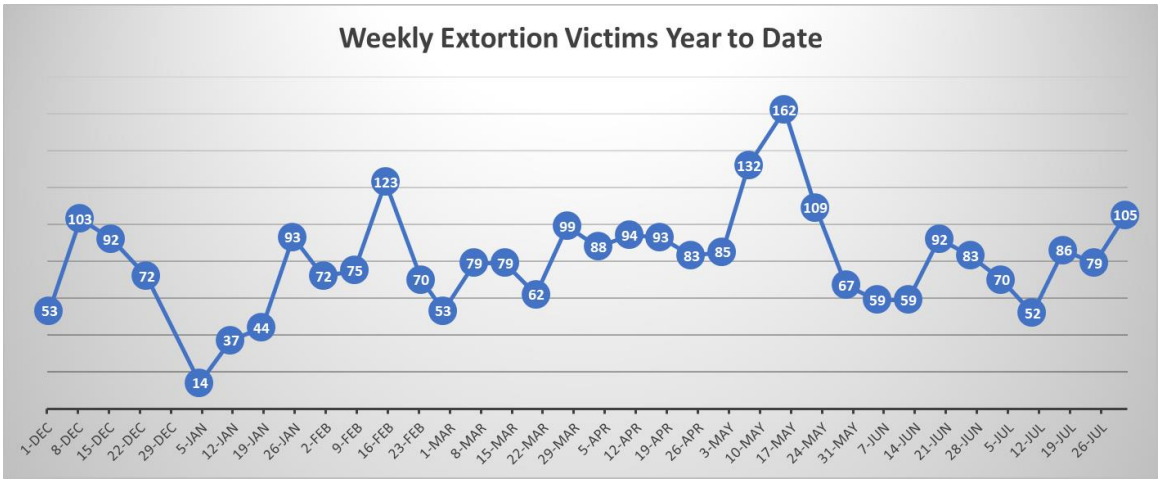
By The Numbers

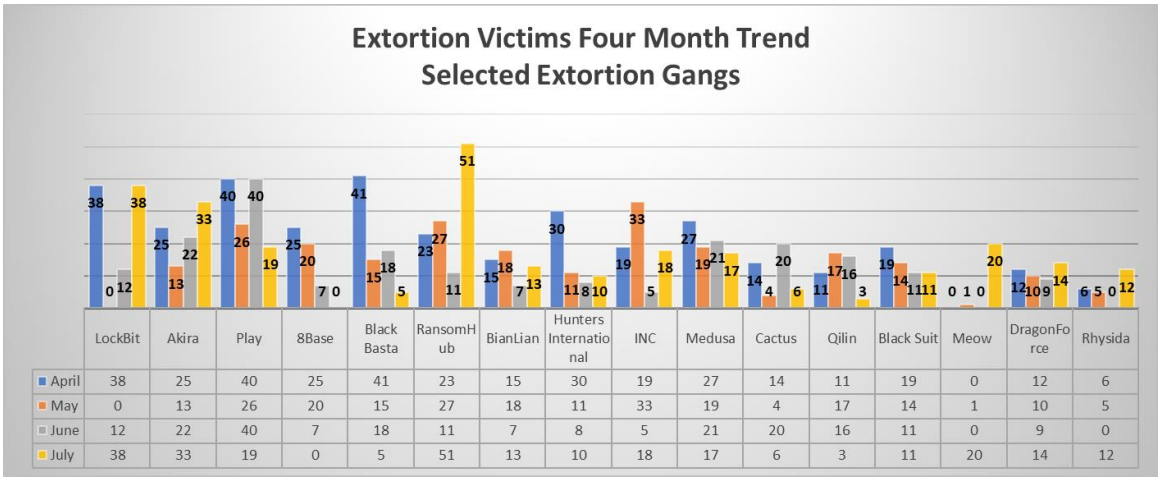
Summarizing incidents in graphical format











	LockBit	Akira	Play	8Base	Black Basta	RansomHub	BianLian	Hunters International	INC	Medusa	Cactus	Qilin	Black Suit	Meow	DragonForce	Rhysida
April	38	25	40	25	41	23	15	30	19	27	14	11	19	0	12	6
May	0	13	26	20	15	27	18	11	33	19	4	17	14	1	10	5
June	12	22	40	7	18	11	7	8	5	21	20	16	11	0	9	0
July	38	33	19	0	5	51	13	10	18	17	6	3	11	20	14	12

New Detection Content

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

- Microsoft App Governance High Severity Alerts
    - This analytic monitors for high severity alerts generated by Microsoft App Governance policies. App governance uses machine learning-based detection algorithms to detect anomalous app behavior in your organization and generates alerts. Beyond this built-in detection capability, you can use a set of default policy templates or create your own app policies that generate other alerts.

- Splunk RCE PDFgen Render
    - This is a hunting search designed to find and discover exploitation attempts against Splunk pdfgen render endpoint which results in remote code execution.

- Splunk RCE via External Lookup Copybuckets
    - This detection logic provides the ability to detect remote code execution attempts against a script named copybuckets present within the splunk_archiver application by calling this script as an external lookup.

- Dumpert LSASS Memory Dumper
    - Looking for indicators of the Dumpert malware used to dump credentials from Lsass memory.

- DS_Poseidon Mac Stealer Indicators
    - This rule searches for indicators related to the Poseidon Mac Stealer. Reference article https://www.malwarebytes.com/blog/news/2024/06/poseidon-mac-stealer-distributed-via-google-ads

---

[i] https://sysdig.com/blog/crystalray-rising-threat-actor-exploiting-oss-tools/
[ii] https://www.bleepingcomputer.com/news/security/fake-crowdstrike-fixes-target-companies-with-malware-data-wipers/
[iii] https://fortinet.com/blog/threat-research/merkspy-exploiting-cve-2021-40444-to-infiltrate-systems
[iv] https://asec.ahnlab.com/en/67502/
[v] https://www.cyfirma.com/research/kematian-stealer-a-deep-dive-into-a-new-information-stealer/
[vi] https://cofense.com/blog/new-malware-campaign-targeting-spanish-language-victims/
[vii] https://www.binarydefense.com/resources/blog/technical-analysis-killer-ultra-malware-targeting-edr-products-in-ransomware-attacks/
[viii] https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/
[ix] https://www.trendmicro.com/en_us/research/24/g/CVE-2024-38112-void-banshee.html
[x] https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust
[xi] https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html
[xii] https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset
[xiii] https://habr.com/ru/companies/f_a_c_c_t/news/831420/
[xiv] https://asec.ahnlab.com/ko/67128/
[xv] https://zscaler.com/blogs/security-research/kimsuky-deploys-translatext-target-south-korean-academia
[xvi] https://blogs.jpcert.or.jp/en/2024/07/attack-activities-by-kimsuky-targeting-japanese-organizations.html
[xvii] https://securelist.com/cloudsorcerer-new-apt-cloud-actor/113056/
[xviii] https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1, https://www.zscaler.com/blogs/security-research/moonwalk-deep-dive-updated-arsenal-apt41-part-2
[xix] https://darkatlas.io/blog/kimsuky-apt-the-trollagent-stealer-analysis
[xx] https://therecord.media/ukraine-scientific-institutions-espionage-russia

[xxi] https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine/