Monthly Threat Intelligence Rollup

DEEP
seas

05/01/24-05/31/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
LockBit Purportedly Unmasked by International Law Enforcement	On 7 May 2024, the U.S. Department of Justice unsealed an indictment purporting to name and shame the creator and operator of the LockBit ransomware group. The ransomware, which has plagued hundreds of companies over the years, is reportedly the work of one Dmitry Yuryevich Khoroshev, who founded the group and developed the LockBit malware no later than September 2019. Numerous other high-profile names who have caused hundreds of millions of dollars' worth of damage to companies worldwide over the past five years, Wazawaka, Bassterlord, and Betterpay for example, are listed in the indictment. The indictment also details cyber criminal intrigue, backstabbing, mob tactics, and other unsavory developments that are not generally associated with the crime of 'hacking' in the public's mind. This demonstrates that these large hacking teams (large being an operative term) operate much like organized crime groups, rather than bored teenagers in their parents' basements. The effects of this indictment are not likely to be immediately damaging, as Russia will refuse to extradite its citizens to the United States or Europe. LockBit will continue operations for at least some time, though a shutdown and rebranding are likely if for no other reason than to attempt to throw investigators off their trail. More worrisome for LockBit is the naming and shaming by the U.S. DOJ. The named individuals will have to look over their shoulders for some time to come, as they will undoubtedly be targeted in real space by competitors and jilted affiliates.[i]
Ascension Healthcare Compromised, Black Basta Group Suspected	In early May 2024, it became apparent that Ascension Healthcare's networks were under active attack by an unspecified threat actor group, almost certainly a ransomware gang. Based on recent publications by CISA, the strongest candidate for the group responsible thus far is the Black Basta ransomware group. DeepSeas has been monitoring the Black Basta ransomware group's targeting and victimology for several years now. Between April 1 and May 10, 2024, the group has claimed a total of 33 victims in multiple verticals, principally manufacturing, construction, logistics, retail, and business services, with only a single healthcare victim. That CISA chose to highlight Black Basta in conjunction with recent reporting about attacks against the healthcare sector is indicative of probable involvement. The group has been highly active and very adaptive so far in 2024, mixing multiple techniques to gain access, although, they apparently always have the goal of installing a Cobalt Strike Beacon as their primary bridgehead into a compromised network. The group has been observed conducting social engineering attacks as well, mass emailing customers with overwhelming amounts of spam before calling and impersonating an MDR provider to convince the victim to download and install remote administration software.[ii]
ZScaler Claims Breach Impacted Test Environment	On 8 May 2024, well-known cloud security company Zscaler announced in a security update on their trust website that investigations were underway of a claim made by a threat actor on Breach Forums that they had obtained unauthorized access to "one of the largest cybersecurity companies." This threat actor, who goes by the moniker IntelBroker, is an established actor who has been active since at least late 2022 and may be operating alone. In the Breach Forums post, IntelBroker does not give the name of the victim company that they allegedly breached; however, they did provide some detail, including the victim company's annual revenue of 1.8 billion USD, which is similar to Zscaler's 2022 revenue earnings of 1.92 billion USD. In their advertisement, IntelBroker stated that the purchaser would have access to "confidential and highly critical logs packed with credentials, SMTP access, PAuth Pointer Auth access, SSL passkeys and SSL certificates." Initial research from Zscaler showed no evidence of such a breach. However, later investigations uncovered an isolated test environment that was exposed to the internet. Thankfully, according to Zscaler, this test environment was not hosted on Zscaler infrastructure and had no connectivity to Zscaler's customer environments. It also was only a single server with no customer data stored within it. According to Zscaler,

	“Zscaler can confirm there is no impact or compromise to its customer, production and corporate environments.” As of this point, that is where Zscaler stands publicly on the matter.[iii]
Stubborn Demon APT Group Abuses Known VIEWSTATE Vulnerability	The Russia-based cyber threat research center, Solar 4RAYS, recently published its findings on an attack on a Russian telecom company near the end of 2023. The company’s network was compromised by an Asian APT group that Solar 4RAYS calls Obstinate Mogwai (or “Stubborn Demon” in English). Stubborn Demon compromised this company by using a well-known vulnerability involving untrusted data deserialization in the VIEWSTATE parameter of the ASP.NET environment. ASP.NET is the open-source web framework created by Microsoft, and VIEWSTATE is the method used by the ASP.NET page framework to preserve page and control values between round trips. Solar 4RAYS has provided the exploitation framework used to abuse the VIEWSTATE vulnerability; these living-off-the land binaries include “Microsoft.Exchange.Management.Powershell.Support.dll,” “Microsoft.Exchange.MessageSecurity.dll,” and “Microsoft.Exchange.UM.UMCommon.dll.” Because this problem has been around for as long as it has, it is likely that this vulnerability may not be patched by Microsoft for some time to come.[iv][v]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
QakBot Integrates Zero-Day Exploit CVE-2024-30051	In early April 2024, Kaspersky Lab researchers decided to investigate the Elevation of Privilege Vulnerability CVE-2023-36033 in Windows, previously discovered as a zero-day exploited in the wild (ITW).	While investigating, they identified a document discussing CVE-2023-36033, containing unusually poor English and exploit code seemingly triggering a different vulnerability. The exploitation process described was identical to that used in CVE-2023-36033, but the vulnerability differed. This would turn out to be CVE-2024-30051, another Windows DWM Core Library Elevation of Privilege Vulnerability. Further analysis of this vulnerability by Kaspersky Lab determined that it was being used to deliver malware, meaning it is actively being exploited ITW, with MALLARD SPIDER's flagship commodity crimeware, QakBot, being prominent among the identified samples. Patches are available, and DeepSeas is attempting to identify recent QakBot dropper documents that have weaponized CVE-2024-30051 for testing.[vi]
Zero Day Reportedly Ignored by Network Manufacturer	After reaching out three times over the course of 30 days, the SSD Secure Disclosure team of researchers continues to receive no response from the affected company, D-Link, about a discovered zero-day vulnerability in one of their products.	This vulnerability, associated with the handling of HNAP login requests in D-Link DIR-X4860 routers, allows attackers to remotely take over these devices and execute commands with root privileges. To do so, the malicious actors send a specially crafted HNAP login request to the router and await response, which returns response data that the attacker can use to create a legitimate password for an admin account. Specifically, the issue seems to lie in the file /bin/prog.cgi, which handles login requests. According to SSD, the vulnerability occurs due to a “lack of proper validation of a user-supplied string before using it to execute a system call.” After exploitation is performed, this means that if the attacker performs a login request, the password "admin" could be used without knowing the real password to avoid proper login verification.[vii]
Linguistic Lumberjack Used to Exploit Cloud Services	After investigation, Tenable Research uncovered a critical memory corruption vulnerability which they dubbed “Linguistic Lumberjack” in Fluent Bit, a logging utility that is frequently used by all major cloud providers.	This security flaw, also known as CVE-2024-4323, is located within Fluent Bit’s built-in HTTP server and could potentially allow for denial-of-service attacks, stolen data, or remote code execution. Due to its deeply involved use in cloud networks such as Google Cloud, Amazon Web Services, and many more, the bug should be taken seriously. Currently, Fluent Bit has not spoken on this matter. Thankfully, however, a patch is currently available for anyone in need of securing their systems. This patch is not run automatically and must be manually updated.[viii]
Unexpected CVE in Courtroom Software	Rapid7 made light of a backdoor designated as CVE-2024-4978 that allows for unauthorized remote access. This backdoor was accidentally implemented into the official 8.3.7 version of JAVS Viewer and would enable attackers to gain full access to an infected	JAVS Viewer is a part of the JAVS Suite 8 portfolio and is made by Justice AV Solutions, a company which is based in the United States and specializes in digital audio-visual recording solutions for environments such as courtrooms, jury rooms, jail and prison facilities, and more. JAVS Viewer is used to open media and log files created by other pieces of JAVS Suite software. It was found that within the JAVS Viewer setup file, a binary named “fffmpeg.exe” would execute upon opening, running a copy of the semi-recent GateDoor/RustDoor family of malware. GateDoor and RustDoor are both Rust-based and written to target MacOS users. Although these backdoors have been previously attributed to the Black Basta

	system.	and ALPHV/BlackCat ransomware operators, there are no signs of connections to these groups in this case. On 27 May, Justice AV Solutions stated that the matter has been investigated, and the malware has been removed in current versions. The remediation steps given were to reimage any endpoints where JAVS Viewer 8.3.7 was installed, reset all credentials, and install the latest version of JAVS Viewer.[ix]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Cuttlefish Malware Targeting Turkish Telecoms Companies	A new malware family sharing significant code overlap with a known Chinese nation-state malware has been identified by Lumen Technologies' Black Lotus Labs. Dubbed Cuttlefish, the malware targets enterprise-grade networking equipment (the so-called SOHO router ecosystem) for the purpose of espionage. The malware has been active since at least July 2023 and operated unabated until April 2024, predominantly targeting Turkish telecommunications providers, or more likely their customers. At least a few victims were U.S.-based, which Lumen suspects is the result of a potential infection at a U.S. datacenter. The malware itself is modular, evasive, and geared towards espionage rather than impact. Cleverly, Cuttlefish remains dormant, sniffing packet traffic until a predefined rule matches on a packet, at which point the malware captures it. In this case, valid credentials were the primary target, though Cuttlefish is capable of much more, including providing a proxy/VPN tunnel to the attackers to log in and exploit purloined credentials. Cuttlefish demonstrates some overlap with the known HiatusRAT malware family, also a known Chinese nation-state malware family, matching up to 77% of the code in some samples according to BinDiff analysis. The HiatusRAT malware was used to target U.S. Department of Defense routers in 2023, seeking information about Taiwanese defense contracting.[x]
APT42 Deploying Two New Backdoors Targeting Cloud Environments	A recent report by Google Threat Research Unit (TRU) described operations conducted by the Iranian state aligned APT42 group, also known as Charming Kitten. The group has been observed conducting enhanced social engineering schemes to steal valid credentials to cloud-based environments, though the group's choice of targets has not changed appreciably. APT42 is still targeting NGOs, media organizations, academic organizations, activists, and legal organizations to seek intelligence on behalf of the Islamic Revolutionary Guard Corps (IRGC). While the tactics were familiar, APT42 has been observed delivering two new backdoor malwares, NICECURL and TAMECAT, both of which are typical infostealers. NICECURL is delivered at the end of a spearphishing chain that begins with a malicious LNK file, while the TAMECAT malware begins with a small VBS downloader script that executes PowerShell to retrieve an encoded TXT file that is then decrypted and executed. This diverse array of tactics speaks to APT42's technical competency, though analysis of these malware families provides ample opportunity for detection. It may be that the APT42 actors are targeting those individuals and organizations that do not prioritize security or do not have the resources to properly detect these threats. It would not be the first time that APT42 has relied on such low-hanging fruit to accomplish their objectives.[xi]
Kimsuky Grows Toolkit with New Linux Backdoor	Symantec's Threat Hunter Team released details of a new backdoor that goes by the name of Gomir. This malware has been seen being used by the infamous North Korea-based Kimsuky APT group, who used the malware in a recent campaign against organizations in South Korea. According to Symantec, Gomir is structurally almost identical to the GoBear backdoor, which has also been used by Kimsuky to target Windows-based devices in the past. As many backdoors do, Gomir also has C2 communication capabilities, along with various commands that can be run through it, such as collecting device information, probing endpoints for further lateral movement, creating and exporting files, and about 13 other commands.[xii]
New Threat Actor Emerges Targeting Multiple Countries	Check Point Research supplied the public with information on 20 May regarding a new threat actor. This adversary, which Check Point has named "Void Manticore," is located in Iran and has connections to the Ministry of Intelligence and Security (MOIS) of Iran. The group is known to carry out destructive wiping attacks combined with influence operations. Void Manticore has also been seen utilizing various online personas, such as "Homeland Justice" when the group targets Albania and "Karma" for attacks carried

	out in Israel. The group also has other malicious connections, such as ties to the group “Scarred Manticore,” with evidence showing that Scarred Manticore would often give access to their previous victims for Void Manticore to continue their work. Void Manticore also has several custom wipers for both Windows and Linux they are known to use, such as Cl Wiper, partition wipers, and BiBi Wiper, which can target both Windows and Linux devices.[xiii]
Operation Diplomatic Specter Haunts World Governments	In a recent research publication by Unit 42, investigators uncloaked a new, active campaign done over the course of a year of analysis which was dubbed “Operation Diplomatic Specter.” The threat actor, tracked by Unit 42 as “TGR-STA-0043,” possesses similar motivations and methods as Chinese APT groups and has been seen targeting political entities in the Middle East, Africa, and Asia since late 2022. Their Chinese affiliations have been determined to be likely due to many signs, such as their shared infrastructure and toolsets with other Chinese APTs. Their targets include organizations such as embassies and military operations, along with individual, high-ranking officials. The threat group also brings new malware to attention, with the group developing two new variants of Gh0st RAT, TunnelSpecter, and SweetSpecter. While both are backdoors, they have key differences. TunnelSpecter, whose name comes from its similarity to Gh0st RAT and its DNS tunneling functionality, has the primary role of creating rogue users. It avoids detection using data encryption and exfiltration over DNS tunneling for increased stealth. SweetSpecter follows its predecessor, Gh0st RAT, by using encrypted zlib packets transmitted over a raw TCP stream and using unique registry keys to store other configuration data.[xiv]
Unfading Sea Haze Emerges from the Mist of the South China Sea	Researchers at Bitdefender Labs have released novel information about a previously unknown threat actor, which Bitdefender has named “Unfading Sea Haze.” This name was given due to the group’s persistence and pursuit of high-level organizations, primarily military and government targets, in the South China Sea. The group has been active but undetected since 2018, which Bitdefender notes is cause for alarm due to how long they have not been discovered, leaving the public wondering what else might have gone undetected. It is believed the group is aligned with China because its geopolitical targeting matches Chinese interests, and it shares tools and techniques with other Chinese threat actors. Their malware arsenal, including the Gh0st RAT family and other custom malware, showcases their focus on flexibility and evasion techniques. The investigation even uncovered a new variant of Gh0st RAT, which goes by the name “SilentGh0st.” This variant happens to be one of the oldest and would eventually evolve into InsidiousGh0st, which led to increased functionality in the malware, particularly where redundancy existed across modules.[xv]

Dark Web Markets

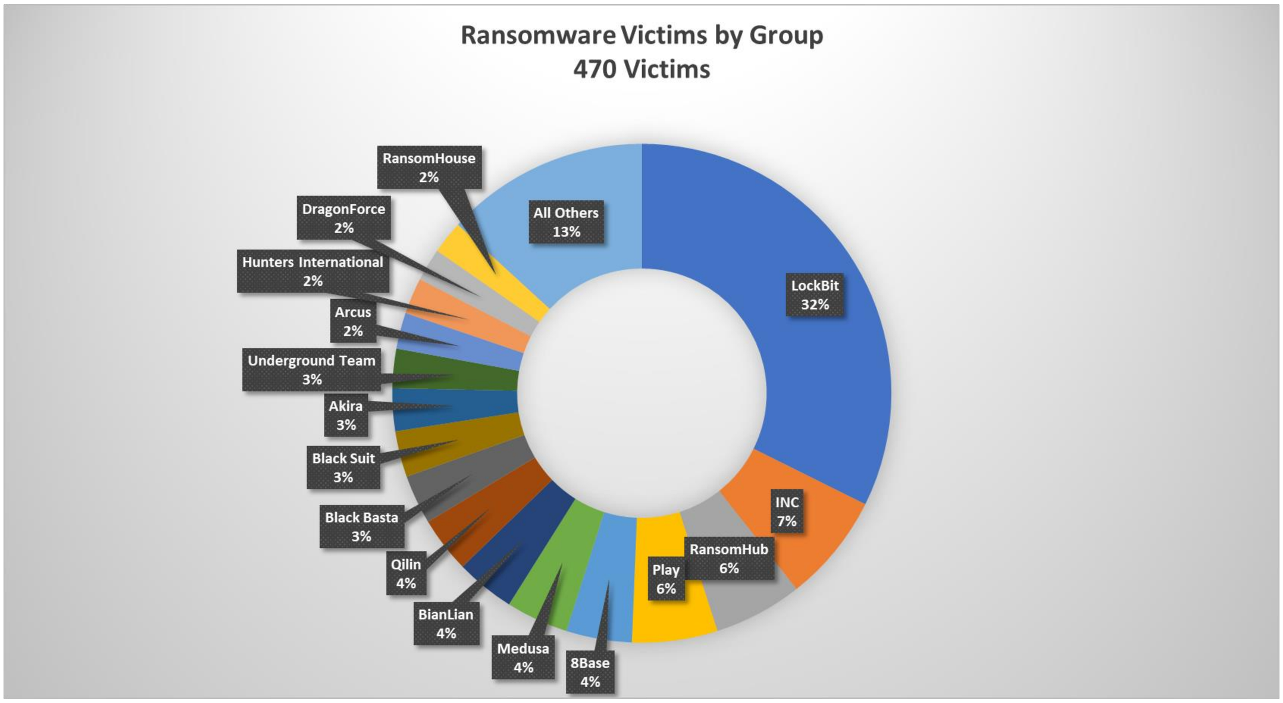
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

Activity	Note
Actor Developments	The long-running Rhadamanthys stealer sales thread was banned from a popular Russian language crime forum for working in the former Soviet Union after an article appeared on a Russian technology site detailing findings by the Russian CTI company F.A.C.C.T. The Ukrainian APT group F.A.C.C.T. called Sticky Werewolf used Rhadamanthys stealer in a cyber espionage campaign in Russia. It is unclear if the seller knew that a Ukrainian APT group was using their stealer.
Data Sale	A crime forum user was observed selling a database of 57,000 patients stolen from a U.S.-based healthcare booking service. They did not name a price.
Access Sale	A crime forum user was selling domain admin access to an unnamed U.S.-based "building manufacturer" with USD 3.9 billion in revenue for USD 10,000. A probable ransomware affiliate/operator expressed interest in purchasing the access.
Tool Sale	A new actor claimed to sell an iMessage 0 click exploit for iOS. The actor did not name a price, but based on public pricing information, the grey market exploit vendor Zerodium would pay upwards of USD 1.5 million for this type of exploit. The actor has already earned a negative review. The forum admin suspended the sale until the actor put up a USD 10,000 vendor bond.
Access Sale	A crime forum access seller was selling domain admin VPN access to a South Korean automobile parts manufacturer with USD 3.7 billion in revenue for USD 10,000.
Actor Developments	An actor on a popular Russian language crime forum was offering to buy access to international shipping companies, claiming access providers could earn more than USD 100,000 per week for access. They did not elaborate further. This comes around the same time Slovak cybersecurity company ESET claimed that the China-linked Mustang Panda group introduced malware over the past five months to gain remote access to “computer systems belonging to cargo shipping companies based in Norway, Greece, and the Netherlands, including some that appeared to be aboard the cargo ships themselves.” While it is unknown if the two incidents are linked, the forum has made efforts in the past to recruit and forge links with Chinese speaking actors.
Access Sale	A notorious actor on a popular criminal forum sold access to what he described as one of the largest cybersecurity companies with USD 1.8 billion in revenue for USD 20,000. The access included SMTP access, SSL passkeys and certificates, and other items. They later identified the company as Zscaler. On 14 May, Zscaler announced, “Following a thorough investigation, Zscaler concluded there is no impact or compromise to our customer, production, and corporate environments. The impact was limited to an isolated single server test environment (without customer data) not hosted on Zscaler infrastructure. The independent third-party IR investigation, which conducted forensic analysis of the incident, is also complete, and the third-party findings are consistent with those of Zscaler,” and considered the incident closed.
Access Sale	An access broker on a Russian language crime forum was selling access to an unnamed company producing UAVs for the European market for USD 10,000.
Access Sale	An actor on a Russian language crime forum was selling domain admin access to a U.S.-based lawyer with USD 210 million in revenue for USD 4,000.
Access Sale	An actor on a Russian language crime forum was selling RDP with root access to a check cashing computer in an Atlanta-area international financial wire service for USD 4,000-5,000. They claimed there are other computers accessible in the network, as well as

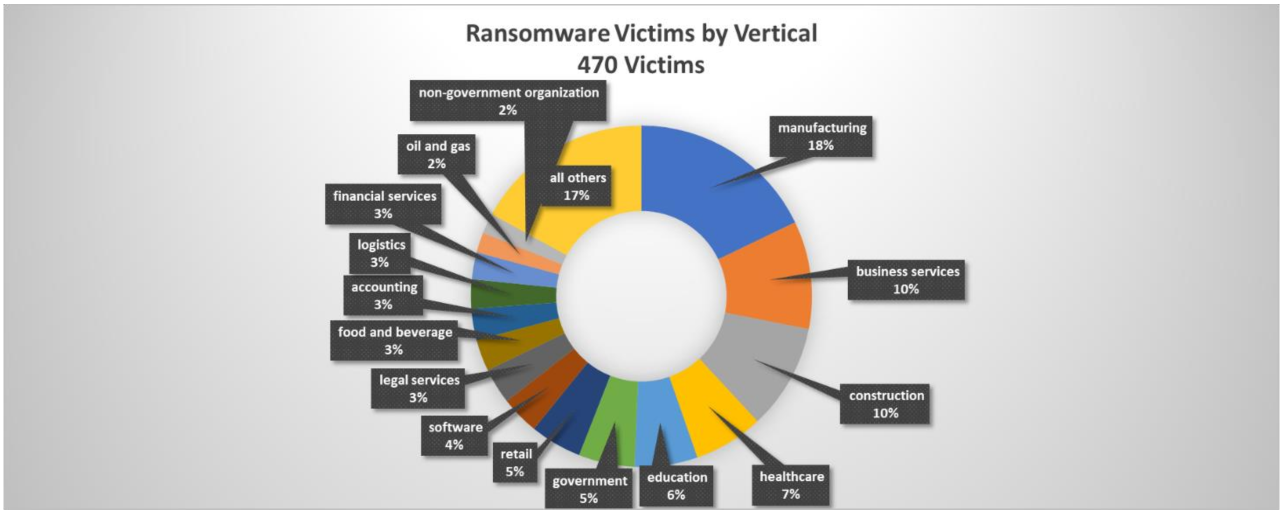
	administrator account access, and provided multiple screenshots to prove access.
Access Sale	An actor on a Russian language crime forum was selling VPN domain admin access to a U.S.-based business services company with USD 2.4 billion in revenue for a best offer or percentage of the ransom.
Access Sale	An actor on a Russian language crime forum was noted selling user access to a U.S.-based company in the "plastics marketplace" with USD 190 million in revenue.
Access Sale	An actor on a Russian language crime forum was selling RDP domain admin access to what they described as one of the largest mining companies in the Democratic Republic of the Congo.
Access Sale	In their first post from an account registered the same day, a new crime forum actor offered sale of access to what they claimed was a major events ticketing database with 560 million users, including full info, the last four digits of credit cards, and event details for USD 500,000. They provided extensive samples to prove their bona fides. Two days later on 28 May, a notorious data hacker posted the exact same advertisement on another Russian language crime forum frequented by malicious actors.
Access Sale	An actor on a Russian language crime forum was selling domain user Citrix access to a network belonging to an American insurance company with more than 7,000 hosts in the domain and more than USD 10 billion in revenue for USD 40,000. The actor provided a poorly redacted screenshot of their PowerShell activity on the network, allowing the victim to be identified.
Tool Sale	An actor on a Russian language crime forum was observed selling what they claimed was a remote code execution (RCE) zero day in Pulse Connect Secure VPN. They claimed to have tested 2,685 IPs, of which 2,102 were vulnerable. They did not describe the vulnerability further and did not name a price.

By The Numbers

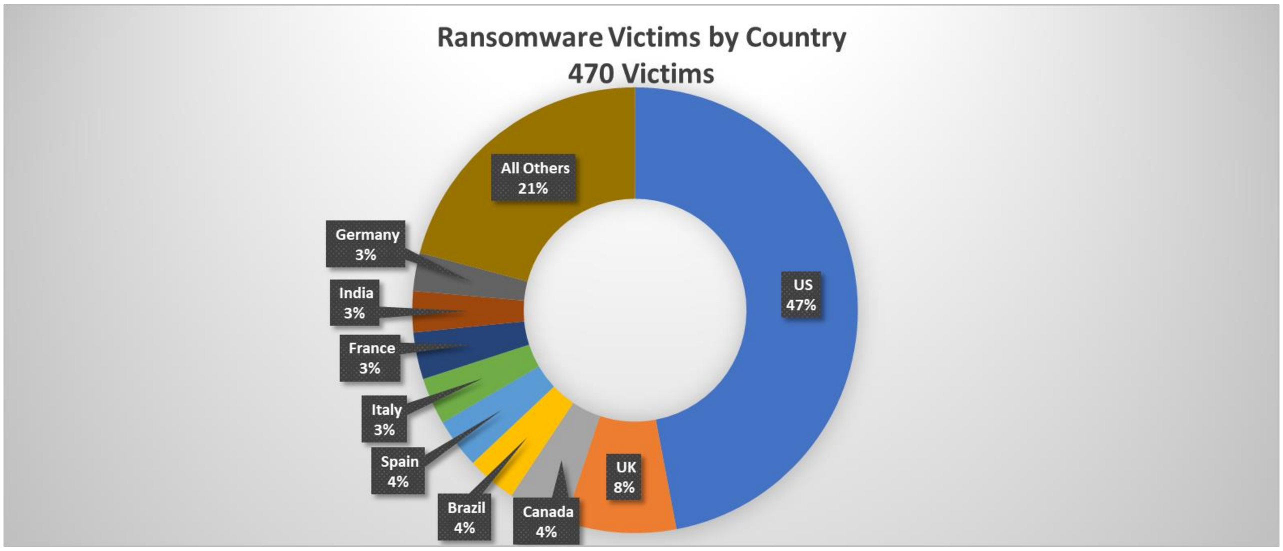
Summarizing incidents in graphical format

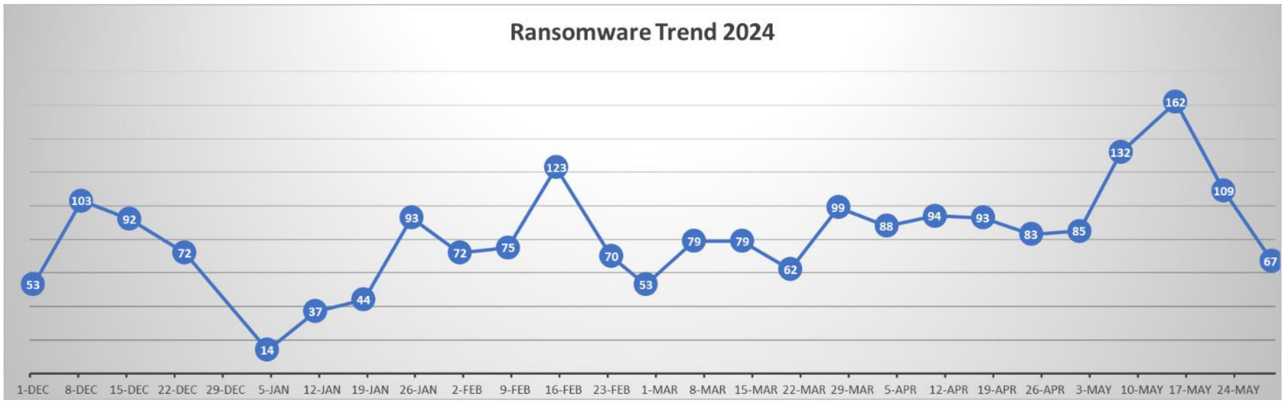


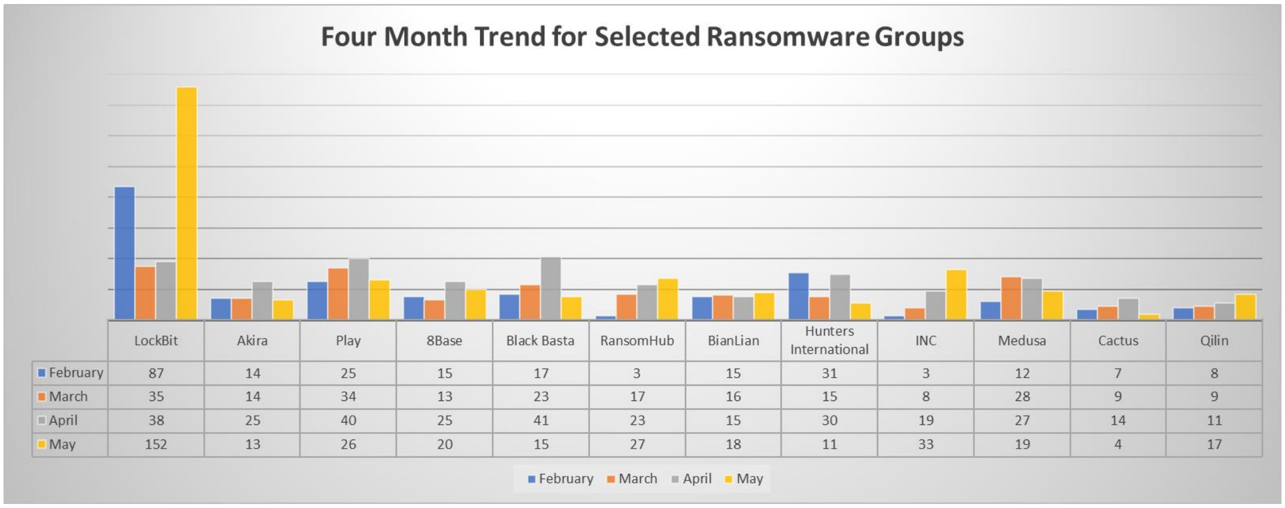
Ransomware Victims by Group
470 Victims



Ransomware Victims by Vertical
470 Victims


Ransomware Victims by Country
470 Victims


Ransomware Trend 2024


Four Month Trend for Selected Ransomware Groups

	LockBit	Akira	Play	8Base	Black Basta	RansomHub	BianLian	Hunters International	INC	Medusa	Cactus	Qilin
February	87	14	25	15	17	3	15	31	3	12	7	8
March	35	14	34	13	23	17	16	15	8	28	9	9
April	38	25	40	25	41	23	15	30	19	27	14	11
May	152	13	26	20	15	27	18	11	33	19	4	17

New Detection Content

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

- ASL AWS Defense Evasion Update CloudTrail
  - The following analytic detects `UpdateTrail` events within AWS CloudTrail logs, aiming to identify attempts by attackers to evade detection by altering logging configurations. By updating CloudTrail settings with incorrect parameters, such as changing multi-regional logging to a single region, attackers can impair the logging of their activities across other regions. This behavior is crucial for Security Operations Centers (SOCs) to identify, as it indicates an adversary's intent to operate undetected within a compromised AWS environment. The impact of such evasion tactics is significant, potentially allowing malicious activities to proceed without being logged, thereby hindering incident response and forensic investigations.
- Identity High Severity Group Policy Action
  - This high severity detection reviews changes on the Domain Controllers using Change Auditor.
- Renamed OpenSSH
  - Threat actors have been seen renaming the OpenSSH tool to try to evade detection and create an encrypted tunnel for remote access. This analytic detects attempts by actors to rename or obfuscate this tool.
- ASL AWS Defense Evasion Stop Logging CloudTrail
  - The following analytic detects `StopLogging` events within AWS CloudTrail logs, a critical action that adversaries may use to evade detection. By halting the logging of their malicious activities, attackers aim to operate undetected within a compromised AWS environment. This detection is achieved by monitoring for specific CloudTrail log entries that indicate the cessation of logging activities. Identifying such behavior is crucial for a Security Operations Center (SOC), as it signals an attempt to undermine the integrity of logging mechanisms, potentially allowing malicious activities to proceed without observation. The impact of this evasion tactic is significant, as it can severely hamper incident response and forensic investigations by obscuring the attacker's actions.
- Identity Account Added to HPA
  - This detection monitors for accounts being added to Highly Privileged Account (HPA) groups in AD.
- Endpoint Anomalous New Process
  - Alert based on frequency of an anomalous number of hosts are detected with a novel process.

[i] https://www.justice.gov/opa/media/1350921/dl?inline

[ii] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

[iii] https://www.securityweek.com/zscaler-confirms-only-isolated-test-server-was-hacked/

[v] https://rt-solar.ru/solar-4rays/blog/4329/

[vi] https://securelist.com/cve-2024-30051/112618/

[vii] https://ssd-disclosure.com/ssd-advisory-d-link-dir-x4860-security-vulnerabilities/

[viii] https://www.tenable.com/blog/linguistic-lumberjack-attacking-cloud-services-via-logging-endpoints-fluent-bit-cve-2024-4323

[ix] https://www.rapid7.com/blog/post/2024/05/23/cve-2024-4978-backdoored-justice-av-solutions-viewer-software-used-in-apparent-supply-chain-attack/s

[x] https://blog.lumen.com/eight-arms-to-hold-you-the-cuttlefish-malware/

[xi] https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

[xii] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/springtail-kimsuky-backdoor-espionage

[xiii] https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/

[xiv] https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

[xv] https://www.bitdefender.com/blog/businessinsights/deep-dive-into-unfading-sea-haze-a-new-threat-actor-in-the-south-china-sea/