Monthly Threat Intelligence Rollup

DEEP seas

4/01/24-04/30/24

TLP:CLEAR

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
MITRE Compromised Via Ivanti Zero-Day Exploit Chain	In April 2024, the MITRE Corporation confirmed that the not-for-profit organization had been compromised by as-yet unidentified threat actors. The attack targeted a network involved in the development of research and prototype technologies, beginning in January 2024, when the actor began reconnaissance of one of the company's VPN appliances. The attack was carried out by chaining together two known Ivanti Connect Secure exploits, at which point the attackers used a session hijacking technique to negate two-factor authentication requirements and moved into MITRE's VMware infrastructure. Despite remediation of the affected Ivanti devices, including full replacement, the attackers skirted past the company's defenses. MITRE has long been a target of nation-state actors, and the use of webshells and implants, rather than more extensive custom toolsets, bolsters the attribution to nation-state actors conducting cyber espionage.[i]
JsOutProx Malware Returns in Wave of Financial Phishing	In late March 2024, VISA published a security alert warning their customers of a new campaign of JsOutProx malware targeting financial institutions and their customers. Though published privately, the alert states that the campaign began on 27 March and is currently ongoing. The JsOutProx malware is a simple first-stage implant capable of permitting the attackers remote access to a compromised machine, along with all that such access entails. This includes payload download and execution, screenshot capture, command execution, and full remote control - including keyboard and mouse. A similar campaign around this time also saw JsOutProx as the first-stage malware in a campaign sending SWIFT and other financially themed emails worldwide, which included a JavaScript file that, when executed, retrieved and executed the JsOutProx payload from a remote GitLab repository. The attackers' end goal is unclear; it is perhaps financially motivated fraud or espionage, though the former seems more likely. It has been years since a major financial institution publicly reported a significant compromise on the scale of those seen (and enabled) in the 2010s. The JsOutProx malware has also received some improvements. Aside from the use of GitLab to host the payload, the malware is now more stealthy, evasive, and provides new options for the end-user to tweak network and command and control configurations to remain hidden and assist in discovery and exfiltration of data of interest.[ii]
DionidasRAT Attacking Linux Installations Worldwide	A recent report by Kaspersky has built upon an October 2023 report by ESET regarding the DionidasRAT malware, which has since been adapted for Linux systems. The original report from ESET noted that the attackers used the Windows version of DionidasRAT to collect hardware specific information of a compromised system. Kaspersky's analysis agrees with this; rather than functioning as a fully featured backdoor, the DionidasRAT appears to be a first-stage implant providing the attackers with access for further mischief. The malware also only targets specific distributions of Linux: RedHat and Ubuntu 16/18, both of which are widely used, rather than the more bespoke Linux distributions like Arch, Kali, and others. This suggests that the operators of the DionidasRAT are not targeting specific industries or applications but rather have broader interests. However, adaptation would be trivial, and other 'flavors' of Linux may also be affected. The targeting noted by Kaspersky is unusual as well; DionidasRAT was observed on systems in China, Taiwan, Turkey, and Uzbekistan, complicating attribution. It may be the work of Chinese state actors, though without further analysis it will remain an open question.[iii]
Backdoor Discovered In xz Utils Package for Linux	In late March, reports began emerging of a potentially catastrophic supply chain attack against a common and popular Linux package, which had the potential to affect every common Linux distribution and some specialized versions. The xz utils package for Linux is considered a core component of Linux, offering data compression and decompression. The backdoor was discovered in operation when an engineer identified excessive CPU cycles being consumed, which turned out to be the backdoor itself. The attack began in 2022, when a developer began adding code to xz utils via Git commits and, over time,

	slowly began to implement the backdoor, supplant the original developer, and lay the groundwork for future attacks by convincing major distributions to update their included xz utils package. Fortunately, the backdoor only made it into development and test builds, rather than major distributions. The attackers did not even include the backdoor code in the official xz utils repo; instead, they included it in precompiled tarballs to avoid detection. While much has been made of the potential for disaster, the effects would have been much the same as the CCleaner compromise in 2015; though millions of devices worldwide were affected, only a tiny fraction of a percent were actually exploited by the nation-state group responsible. There are only so many trained and cleared operators to exploit access. This supply chain attack bears many of the same hallmarks of the CCleaner attack, though much improved in stealth and sophistication.[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
ArcaneDoor Espionage Campaign Both Novel and Evasive	In early 2024, Cisco Talos researchers identified a unique malware campaign, very likely the work of skilled and well-provisioned nation-state actors. The campaign targeted perimeter devices (ASA for example) from multiple vendors belonging to multiple government networks.	The campaign identified by Cisco Talos is global in scale and makes use of two unique malwares not seen before. Initial access to the perimeter devices is unknown. Once the attackers gained access, an in-memory implant dubbed Line Dancer was installed, giving the attackers the ability to execute commands. These commands consisted of evasive maneuvers and establishing an unauthenticated backdoor. The second component, Line Runner, is the group's persistence mechanism that functions as a secondary backdoor in the case of detection and attempted remediation. Two CVEs (CVE-2024-20359 and CVE-2024-20353) were exploited by Line Runner to execute the payload. In at least one instance, Line Runner was used to access and retrieve information staged by Line Dancer. By working in concert, these two malwares provided the attackers with stealthy, persistent access to government-owned perimeter devices. Attribution remains unknown; researchers did not provide any details on targeting, suggesting only that Line Dancer and Line Runner were the work of nation-state actors without naming names. Without targeting data, little in the way of attribution can be done.[v]
Newly Discovered Kapeka Malware Targets Eastern Europe	WithSecure Intelligence has recently released information on a novel backdoor dubbed "Kapeka," which has been utilized in targeted attacks across Eastern Europe since the middle of 2022.	Exhibiting advanced functionalities, Kapeka operates as a multi-purpose tool, providing initial access and enabling long-term control of compromised systems. Analysis reveals connections between Kapeka, GreyEnergy, and Prestige ransomware attacks, suggesting affiliation with the Sandworm group linked to the Russian GRU. Kapeka's deployment coincides with the ongoing Russia-Ukraine conflict, with indications of its involvement in intrusions leading to Prestige ransomware deployment. Likely succeeding GreyEnergy, Kapeka underscores Sandworm's persistent cyber threat in the region.[vi]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
PlugX Worm Variant Proves a Headache for Nation-State Actors	An older variant of the PlugX malware often utilized by Chinese nation-state actors operated for nearly five years before Sekoia researchers succeeded in sinkholing the botnet's command and control (C2) server. Following months of analysis, Sekoia researchers determined that the PlugX malware, modified by the nation-state operators to be self-propagating, had infected nearly 100,000 unique systems worldwide. While other botnet malware such as Mirai, Conficker, and others boast numbers in the millions, this network of PlugX infections is one of the largest attributed to a nation-state actor. Interestingly, the botnet was considered 'dead' by Sekoia researchers, as the Chinese actors had failed to disable it following the conclusion of their operations. The so-called worm capability was added in 2020 and rapidly got out of control by spreading too far and too quickly, causing the operators to abandon their C2 infrastructure. By the time Sekoia sinkholed the infrastructure, the incoming connections approached 2MB/sec, a huge volume of traffic. Cleverly, Sekoia researchers developed a sanitization method to not only remove the infection but also disable any subsequent reinfections by targeting any infected USB drives connected to the infected system. Despite this, other C2 servers remain active, and as worm-capable malware has proven remarkably resilient against remediation, this PlugX variant is likely to remain around for many years to come.[vii]
FIN7 Swims Against the Current into a New Attack Vector	On the evening of 17 April, analysts at Blackberry published the findings of a new phishing campaign ran by FIN7, a Russian APT group that has been active since 2013. Traditionally, FIN7 are known for casting a wide net for their targets, installing ransomware onto any device they could to get quick cash. However, in recent years, they have been targeting large corporations, with their most recent target being a large automotive manufacturer based in the United States. As with most phishes, FIN7 uses a spear phishing email to lure a potential victim to open and run a malicious attachment that will infect the machine. The campaign's end goal was to install the Carbanak backdoor onto a victim's device and gain an initial foothold into their environment. Carbanak is traditionally known to be delivered via spear phishing, so this commonality makes sense.[viii]
Muddled Libra Targeting SaaS, Cloud Providers	A new report by Palo Alto Unit 42 details recent operations by the Muddled Libra group (aka SCATTERED SPIDER), notorious for their compromise and ransoming of several high-profile Las Vegas casinos. The group has improved their tactics, adopting cross-tenant impersonation attacks in Okta using stolen administrator credentials before elevating their permissions to permit access to security tools (security-as-a-service, or SaaS) and cloud service provider accounts. This points to the group adopting a long-term approach to their targets, not relying simply on stolen credentials to gain access but taking their time to conduct proper reconnaissance, followed by compromise, lateral movement, and asset discovery, before exfiltrating data. A preferred method observed by Unit 42 is the use of VM snapshots of devices of interest, a tactic which is unlikely to be detected as snapshot creation is common in the environments where Muddled Libra operates. Exploitation of SaaS is done to elevate privileges and collect credentials and other sensitive information for exfiltration and further exploitation, as is compromise of cloud service provider accounts (aka AWS). It should be stated that no evidence of vulnerability exploitation was noted; rather, abuse of valid credentials appears to be the tactic of choice in these cases. Fortunately, there are numerous methods to detect the creation of new users, VM snapshots, and other parts of the Muddled Libra attack chain.[ix]

Latrodectus Malware a Potential Successor to IcedID Loader	According to research by Proofpoint's Threat Research Team, a new malware family dubbed Latrodectus, which first appeared in October 2023, is a new loader used as a first-stage implant or downloader in phishing campaigns. Analysis of the Latrodectus malware has determined that it is likely the work of the LUNAR SPIDER group, known for their flagship product the IcedID (aka Bokbot) loader. Thus far nearly a dozen discrete phishing campaigns have been identified by Proofpoint, including some operated by the TA577 and TA578 groups, though only TA578 has maintained their use of it; TA577 briefly used Latrodectus before switching back to the Pikabot loader. Analysis of the malware itself shows little to no significant overlap with IcedID's code base, though the infrastructure overlap, bot naming conventions, and campaign IDs are very strongly correlative to previous IcedID operations. In addition, new features are present including robust anti-VI and anti-analysis checks. Despite the revamp and new features, the malware functions much the same as the group's original IcedID offering, acting as a loader for follow-on payloads as well as collecting and exfiltrating sensitive information including the computer name, credentials, browser cookies, screenshots, file and process lists, etc. Given that the malware appears to be in operation though with a somewhat limited set of capabilities compared to IcedID (Latrodectus does not collect browser credentials, passwords, etc.) it is likely that further development over the coming months will see the Latrodectus malware's capabilities improve markedly.[x]
Operation FlightNight Strikes India Government, Energy Targets	In early March 2024, an unattributed attacker began targeting Indian entities with a modified version of an open source infostealing malware in a campaign dubbed 'Operation FlightNight.' The name stems from the malware's use of the commercial messaging application Slack for command and control (C2) communications. The use of Slack is the most notable aspect of the malware. Rather than using Slack for all C2 communications, stolen data is exfiltrated elsewhere, and only small amounts of data are sent to Slack; victims, file paths, timestamps, and download URLs for stolen data are sent. This reduces the size of the Slack traffic, making it more likely to blend in, especially in environments where Slack is already present. The attack made use of a typically complex but simple tactic: spearphishing with decoy PDF documents inside an ISO file, as well as a LNK file. The inclusion of multiple methods to trigger an attack is unusual, suggesting that either this campaign was of importance to the attackers or that time was of the essence. Given that the attackers targeted Indian government agencies responsible for telecommunications, national defense, energy, oil and gas, and basic governance, the attackers were most likely intent on espionage.[xi]

Dark Web Markets

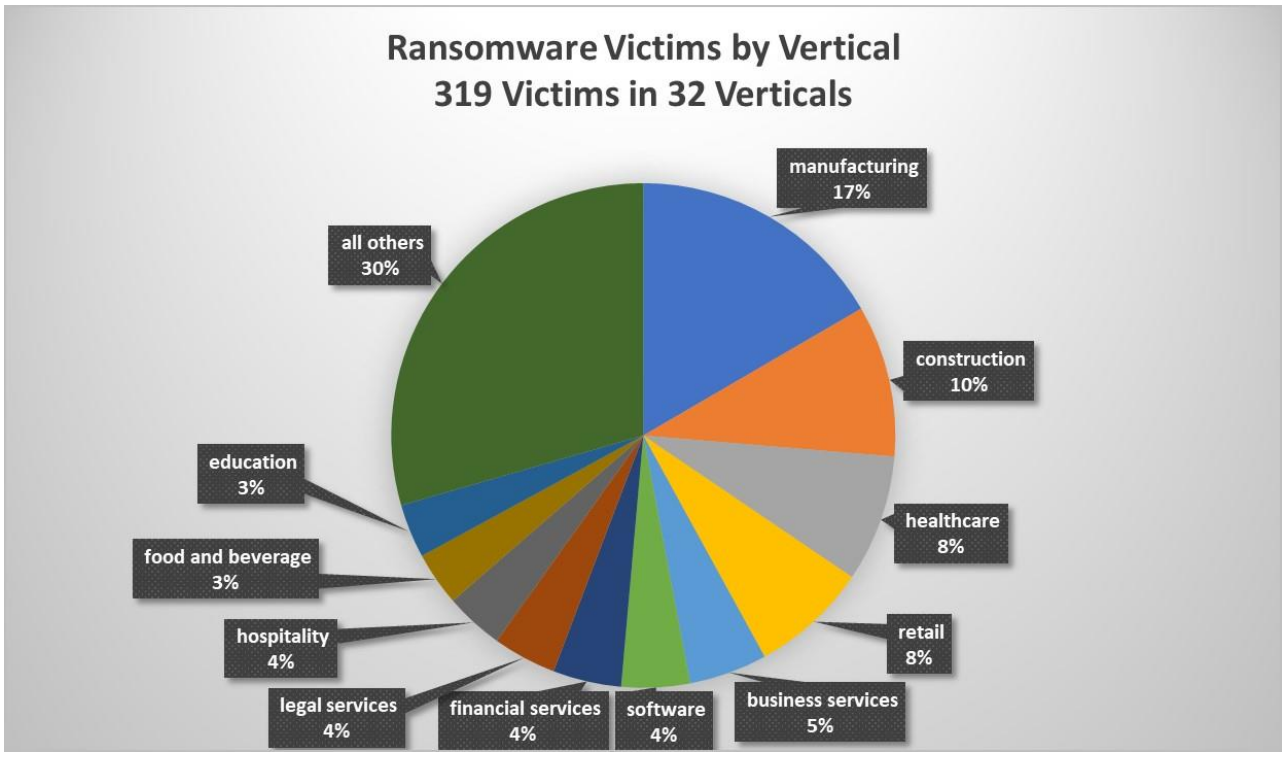
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

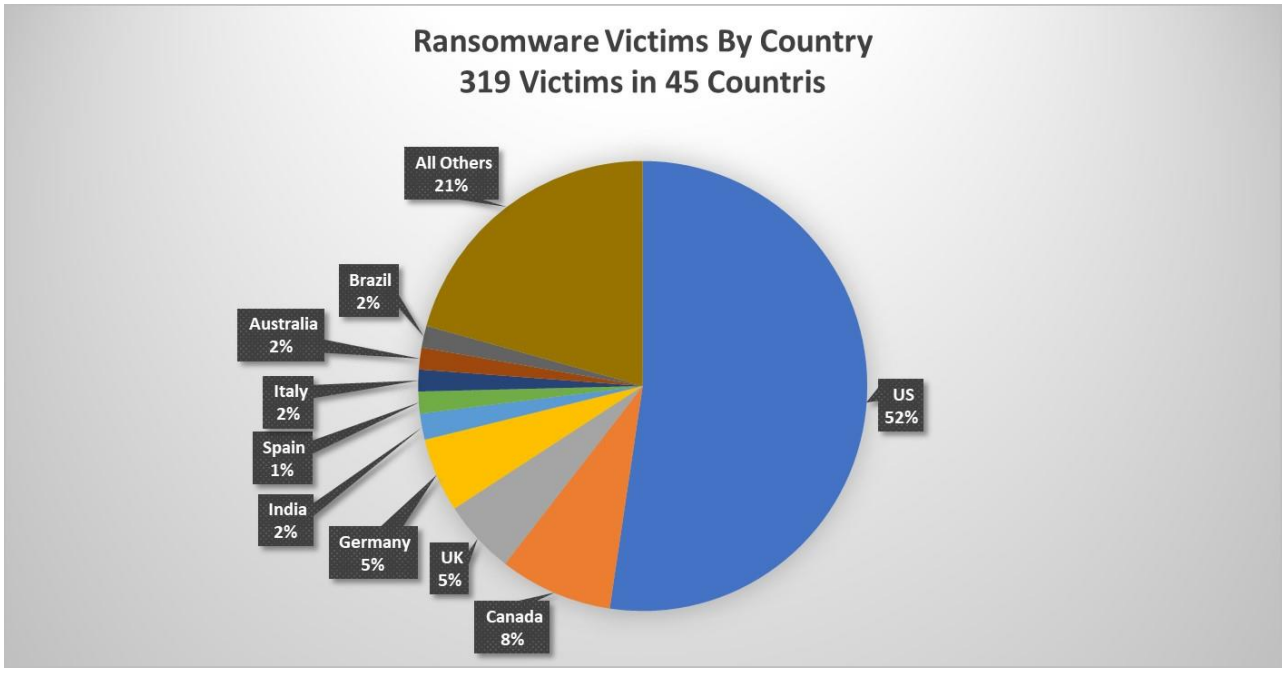
Activity	Note
Actor Developments	A moderator on the Russian language RAMP crime forum was advertising to buy accesses with what could be considered unusual stipulations, including: • U.S. accesses only (Actors will usually take accesses from almost any Western nation.) • No networks protected by Sentinel One • Very specific industry verticals (lawyers and non-ISP IT technology companies) • Critical infrastructure, military infrastructure, and healthcare (Three areas most ransomware operators profess to stay away from, especially after Colonial Pipeline.) The unusual targeting list may suggest that they are engaging in IP theft and economic sabotage against the United States, and while they are at it, some ransomware on the side. However, the primary purpose appears to be some sort of tasking.
Access Sale	An actor on the Russian language XSS crime forum is selling RDP access to the domain controller of an unnamed large bank in a "Tier 1 EU country." He did not show any proof of access or elaborate on the identity of the bank.
Access Sale	An actor on the XSS crime forum was selling RDP access to a New York based private equity company with USD 3.5 billion in assets under management for USD 2,000.
Access Sale	An actor on the RAMP crime forum was selling domain and local admin access to a U.S. based enterprise with 10,835 hosts in five trusts and USD 546.1 million in revenue. He would not name the industry vertical or a price.
Access Sale	An actor on the XSS crime forum was selling domain admin RDP access to a U.S. based manufacturer with USD 978.8 million in revenue for USD 6,000. The victim remains unidentified.
Access Sale	An actor on the XSS and Exploit crime forum was selling local admin access to an enterprise in the grocery retail vertical with USD 776.6 million in revenue for USD 2,000.
Access Sale	An actor on the XSS crime forum was selling local admin access to a manufacturing enterprise with USD 2.8 billion in revenue for USD 4,000.
Access Sale	An actor on the XSS crime forum attempted to sell Citrix access to a pharmaceutical company to another member. The sale fell through after the seller refused to use the automated escrow system to conclude the deal. In private messages provided by the buyer, the seller revealed the victim's identity and provided a screenshot of himself logged into the company's systems.
Access Sale	An actor on the Exploit crime forum was selling Citrix domain user access to a China based pharmaceutical company with USD 945 million in revenue for a buy now price of USD 3,500.
Tool Sale	A new actor on the XSS crime forum was selling what they claim is a zero click RCE in Apple iMessage for USD 2 million. They did not provide any proof or elaborate further about the nature of the exploit. Zerodium will pay up to USD 1.5 million for a zero click RCE in iMessage, making it curious as to why the actor just doesn't sell it to them if the exploit is legitimate.
Access Sale	An actor on the XSS crime forum was selling what he claimed was around 500 GB of data taken from a credit firm's database. Supposedly, the data consists of 2.9 billion lines of social security numbers and 900 million lines of personal information. He posted two screenshots of what is supposed to be the data and offered to provide 5 million sample lines to interested parties. He is asking USD 200,000 to USD 1,000,000 for the data.
Access Sale	An actor on the XSS crime forum was selling RDP local admin access to a U.S. based enterprise in the industrial machinery vertical with USD 4.8 billion in revenue for a buy now price of USD 10,000.

Access Sale	An actor on the XSS crime forum was selling VPN Citrix access to a call center employee with access to the employee tools. The SSO domain login and 2FA were supposedly included. Screenshots provided by the actor suggest that AnyConnect access was also included. Price was USD 12,000.
Access Sale	An actor on the Exploit crime forum was selling RDWeb user access to a fertility clinic with USD 19.5 million in revenue for USD 800.
Access Sale	An actor on the RAMP forum sold VPN access to an enterprise in the sports teams & leagues vertical with USD 519 million in revenue.
Access Sale	An actor on the XSS crime forum is selling Palo Alto Global Protect access to a Vietnam-based enterprise in the airlines, airports, and air services vertical with more than USD 2 billion in revenue for USD 800.
Access Sale	An actor on the XSS crime forum sold RDP domain admin access to a U.S. based manufacturing enterprise with 11,029 hosts on the network and USD 10.3 billion in revenue. He was also selling access to a Citrix RDP domain admin access to a U.S. based media and internet company with USD 652.9 million in revenue and 711 hosts on the network.
Access Sale	An Exploit crime forum access seller was selling RDP domain admin access to a France-based outsourcing company with USD 830.2 million in revenue for USD 500.
Access Sale	An XSS crime forum actor sold 60 GB of patient data stolen from a Columbia, Maryland based laboratory, including name, address, phone number, date of birth, and full social security number.

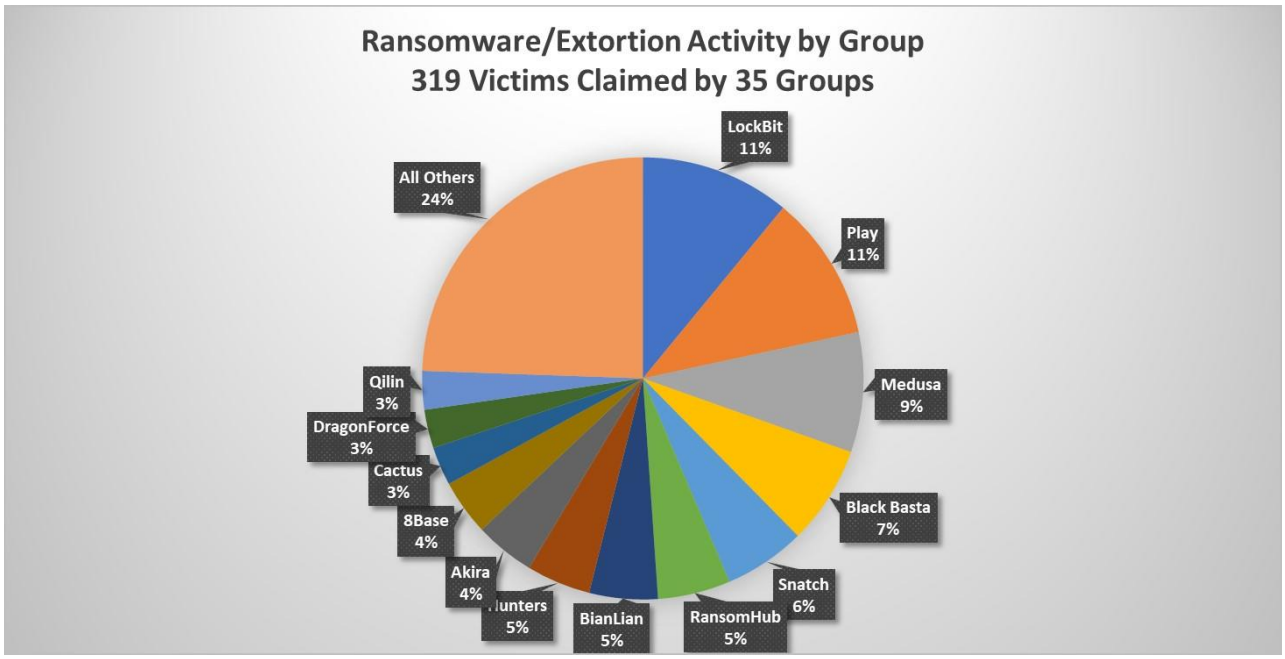
By The Numbers

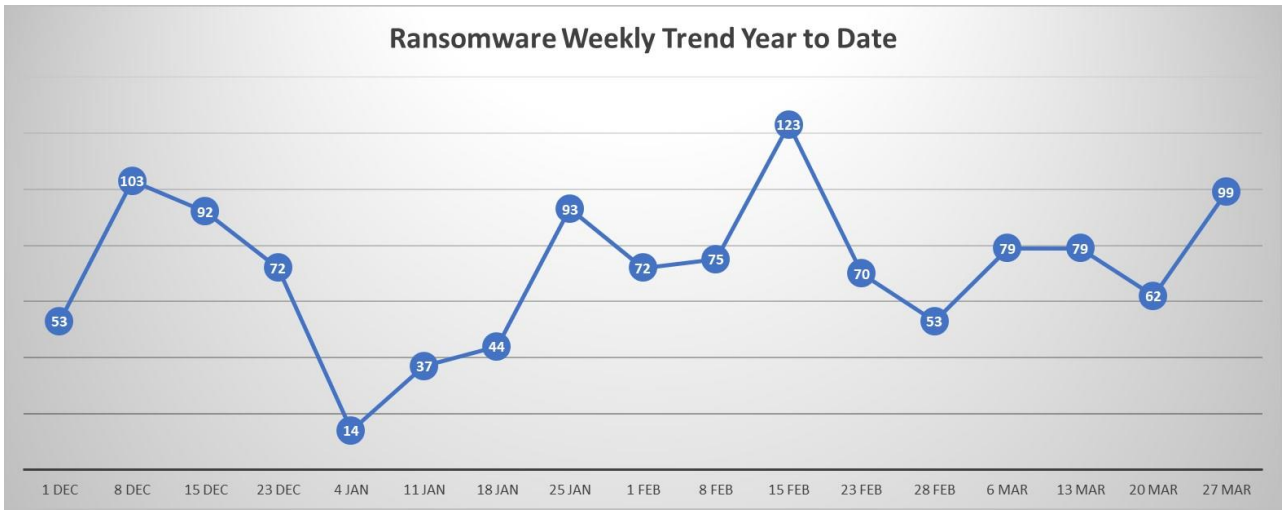
Summarizing incidents in graphical format

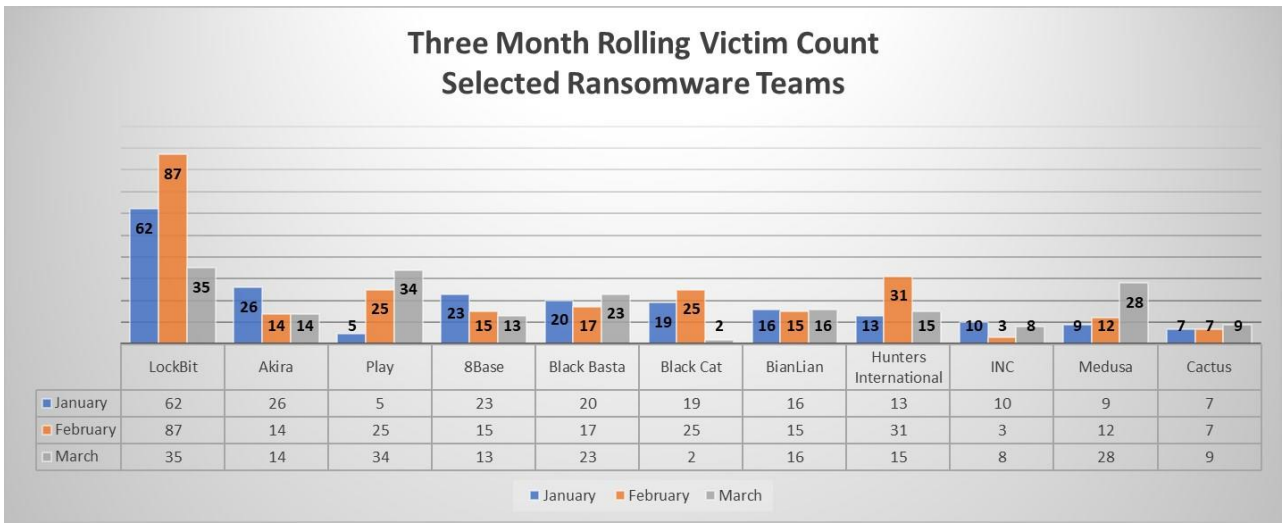




TLP:CLEAR







	LockBit	Akira	Play	8Base	Black Basta	Black Cat	BianLian	Hunters International	INC	Medusa	Cactus
January	62	26	5	23	20	19	16	13	10	9	7
February	87	14	25	15	17	25	15	31	3	12	7
March	35	14	34	13	23	2	16	15	8	28	9

TLP:CLEAR

New Detection Content

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

Name	Description
Okta IDP Lifecycle Modifications	This detection identifies modifications to Okta Identity Provider (IDP) lifecycle events, such as creation, activation, deactivation, and deletion of IDP configurations. Monitoring these events is crucial for maintaining the integrity and security of authentication mechanisms within an organization. By detecting unauthorized or anomalous changes, organizations can quickly respond to potential security breaches or misconfigurations, ensuring that their identity management systems remain secure and operational.
Okta Unauthorized Access to Application	This search detects instances where a user attempts to access an Okta application that has not been assigned to them. Such unauthorized access to applications poses a significant security risk, potentially leading to the exposure of sensitive information, disruption of services, and breaches of data protection laws. Ensuring that only authorized users have access to applications is crucial for maintaining a secure and compliant IT environment.
Zscaler Privacy Risk Destinations Threat Blocked	This analytic is designed to identify blocked destinations within a network deemed as privacy risks by Zscaler. Utilizing Splunk search functionality, it processes web proxy logs, focusing on entries marked as Privacy Risk. Key data points such as device owner, user, URL category, destination URL and IP, and action taken are analyzed to enumerate the privacy risk destinations. This anomaly-type detection aids in monitoring and managing privacy risks, promoting a secure network environment.
Windows AppLocker Privilege Escalation via Unauthorized Bypass	The following analytic utilizes Windows AppLocker event logs to identify attempts to bypass application restrictions. AppLocker is a feature that allows administrators to specify which applications are permitted to run on a system. This analytic is designed to identify attempts to bypass these restrictions, which could be indicative of an attacker attempting to escalate privileges. The analytic uses EventCodes 8007, 8004, 8022, 8025, 8029, and 8040 to identify these attempts. The analytic will identify the host, full file path, and the target user associated with the bypass attempt. These EventCodes are related to block events and focus on five attempts or more.
Windows AppLocker Execution from Uncommon	This analytic is designed to identify executions of applications or scripts from uncommon or suspicious file paths, which could be indicative of malware or unauthorized activity. By leveraging a simple statistical model, the query analyzes the frequency of application executions across different file paths. It calculates the average

Locations	(avg) number of executions per file path and uses the standard deviation (stdev) to measure the variation or dispersion of the execution counts from the average. A file path is considered uncommon or suspicious if the number of executions from it is significantly higher than what is expected based on the calculated average and standard deviation. Specifically, the analytic flags any file path from which the number of executions exceeds the upper bound, defined as the average plus two times the standard deviation (avg+stdev*2). This approach helps in pinpointing anomalies in application execution patterns, potentially uncovering malicious activities or policy violations.
Okta Multiple Users Failing to Authenticate from Ip	This analytic identifies instances where multiple users (more than 10 unique accounts) have failed to authenticate from a single IP address within a short time span (five minutes) within an Okta tenant. Such a pattern can be indicative of malicious activities, such as brute force attacks or password spraying attempts. Identifying and responding to such patterns promptly is crucial to prevent potential account compromises and unauthorized access to organizational resources. If the detection is a true positive, it suggests that an external entity is actively trying to breach security by targeting multiple user accounts.
Windows SqlWriter SQLDumper DLL Sideload	The following analytic identifies the abuse of SqlWriter and SQLDumper executables to sideload the vcruntime140.dll library. This technique is commonly used by adversaries to load malicious code into a legitimate process. The analytic searches for EventCode 7 from Sysmon logs where the Image is either SQLDumper.exe or SQLWriter.exe and the ImageLoaded is vcruntime140.dll. The search also filters out the legitimate loading of vcruntime140.dll from the System32 directory to reduce false positives.
Windows Unsigned MS DLL Side-Loading	The following analysis identifies potential DLL side-loading instances involving unsigned DLLs with a company detail signature mimicking Microsoft. This technique is frequently exploited by adversaries to execute malicious code automatically by running a legitimate process. The analytic involves searching Sysmon logs for Event Code 7, where both the `Image` and `ImageLoaded` paths do not match system directories (`system32`, `syswow64`, and `programfiles`). Additionally, it verifies whether the loaded DLL is signed and checks if the folder paths of the `Image` and `ImageLoaded` are identical. This anomaly detection mechanism serves as a valuable indicator for identifying suspicious processes that load unsigned DLLs. Add other paths based on org hunting.

[i] https://medium.com/mitre-engenuity/advanced-cyber-threats-impact-even-the-most-prepared-56444e980dc8
[ii] https://www.bleepingcomputer.com/news/security/visa-warns-of-new-jsoutprox-malware-variant-targeting-financial-orgs/

[iv] https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/
[v] https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
[vi] https://labs.withsecure.com/publications/kapeka
[vii] https://blog.sekoia.io/unplugging-plugx-sinkholing-the-plugx-usb-worm-botnet/
[viii] https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry
[ix] https://www.bleepingcomputer.com/news/security/visa-warns-of-new-jsoutprox-malware-variant-targeting-financial-orgs/
[x] https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice
[xi] https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign