Monthly Threat Intelligence Rollup

DEEP seas

03/01/24-03/31/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Magnet Goblin Exploiting Multiple Vulnerabilities	Beginning in early January 2024, researchers at Check Point began observing multiple campaigns by a threat actor dubbed Magnet Goblin. This financially motivated group has been observed making use of multiple zero-day and n-day vulnerabilities, including those in Ivanti Connect Secure VPN, Magento, Qlink Sense, ConnectWise ScreenConnect, and Apache ActiveMQ. The group has adopted at least eight vulnerabilities since it began operations in January 2022, often within days of a public proof of concept (PoC) being released. In addition to vulnerability exploitation, the group utilizes their own malware families (the Windows-based NerbianRAT and a Linux version of NerbianRAT), giving the group wide reach. More interestingly, the WARPWIRE RAT is also attributed to Magnet Goblin activities, hinting either at overlap between multiple actors utilizing the same tool, or the emergence of a new malware-as-a-service (MaaS) operator.[i]
Phishing Campaign Distributing VCURMS, STRAAT Malware	On 12 March 2024, researchers at Fortinet released a report on a recent phishing campaign delivering the STRAAT remote access trojan (RAT) and the new VCURMS RAT. The attack begins with a phishing email linking to a malicious JAR file hosted on Amazon Web Services (AWS) or GitHub. Annoyingly, the use of AWS and GitHub to store and distribute their malware complicates network-based detection and the process of retrieving samples for analysis. However, the malware is protected (re: obfuscated) using the Branchlock obfuscator, which provides some detection opportunities. The malware functions as a fully featured infostealer. System information, screenshots, Discord tokens, Steam tokens, and browser information are targeted by the operators of this campaign, suggesting that the group operates as an initial access broker at worst. Discord and Steam tokens often bring a high price on cyber criminal marketplaces, though the use of financial-themed phishing is curious.[ii]
WhiteSnake Stealer Sheds Its Skin	On 18 March 2024, the SonicWall Capture Labs threat research team disclosed a new variant of WhiteSnake Stealer, which, while under less protection through obfuscation, has even more potential to be dangerous. The stealer has been previously known for stealing data from compromised systems, such as web browser data and cryptocurrency wallets. Now, it is capable of that and much more, such as sandbox detection, persistence, screenshotting, keylogging, recording audio through the victim's microphone, recording video through the victim's webcam, and remote access. The attacker performs these features at will through a remote console, such as the "SCREENSHOT" command to take a screenshot of the victim's screen and "MICROPHONE" to record sound from the victim's microphone. After the data is collected, WhiteSnake will then send the data to their C2 infrastructure for later use, in typical malware fashion.[iii]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
The Mystery of CHAVECLOAK Uncovered	On 4 March, the FortiGuard Labs team at Fortinet discovered a new Trojan targeting banking organizations in Brazil in order to steal any valuable information that may be linked to their financial transactions.	This Trojan, named CHAVECLOAK by Fortinet, works by first being delivered to the victim through a phishing email containing a PDF document with a malicious link. This document, written in Portuguese, claims the victim must sign documents related to a "contract." The link leads the victim to a fake DocuSign page, where clicking the link to sign the documents downloads a ZIP file containing the CHAVECLOAK installer. After unpacking the ZIP file and running the installer, DLL sideloading is utilized, a technique used to evade detection from Windows to perform malicious actions on a target. The DLL file executed using DLL sideloading, in this case Lightshot.dll, is the CHAVECLOAK trojan. Once fully operational, CHAVECLOAK will go through the following steps. First, it will gather details about the file system and the root directory. Then, the Trojan will confirm that it will automatically execute when the affected endpoint is logged into. It then will send the collected data back to its associated C2 server, which will confirm the victim is in Brazil and that it is indeed a financial institution before continuing. Next, actions on objectives are taken, and the malware attempts to steal the victim's credentials, along with other nefarious actions such as logging keystrokes, showing the victim malicious pop-up windows, monitoring communication with other financial companies for further pivoting, and more. CHAVECLOAK will then finally send all the sensitive data collected once again to its C2 server, where the credentials may be used to escalate privileges, pilfer funds from affected accounts or threaten to release their data for ransom.[iv]
Multiple JetBrains TeamCity Vulnerabilities Lead to InfoSec Drama	In mid-February 2024, security firm Rapid7, well known for their work identifying and reporting vulnerabilities, identified two serious vulnerabilities in JetBrains TeamCity software, a popular build management and continuous integration platform regularly used in corporate environments.	The vulnerabilities, CVE-2024-27198 and CVE-2024-27199, are both authentication bypass vulnerabilities that would permit an attacker to gain full control of the TeamCity server for their own malicious purposes. While vulnerability disclosures are common enough, and the timeline reported by Rapid7 follows most vulnerability disclosure timelines, the choice by JetBrains to release updates silently apparently rankled Rapid7, which released the full details of the vulnerabilities and steps to reproduce. This disclosure by Rapid7 makes exploitation for even low-skilled actors trivial and has led to some debate. The 'sunlight is the best disinfectant' mindset does have its merits, though silent patching also has some merits.[v]
The Agenda for Qilin Ransomware Has Changed	Trend Micro has recently detected an updated version of Qilin ransomware utilizing the Rust programming language, tracked internally as Agenda	The Agenda ransomware group, also known as Water Galura to Trend Micro, has made significant changes to Qilin, such as new command line capabilities, new PowerShell scripts for lateral movement across vulnerable servers, using printers on a victim's network to print ransom notes, terminating VMclusters, along with exploiting vulnerable drivers for defense

	ransomware by Trend Micro.	evasion. The ransomware group behind Qilin uses Remote Monitoring and Management (RMM) tools, as well as Cobalt Strike for the deployment of the Qilin ransomware binary. As for the Qilin ransomware executable itself, the file propagates via PsExec and SecureShell, while using vulnerable SYS drivers for defense evasion. The threat group behind Qilin is known to target countries such as the United States, Argentina, Australia, and Thailand, with its main industry targets being both the finance and law sectors.[vi]
APT33's FalseFront Backdoor Targeting Human Resources Departments	Beginning in December 2023, the Iranian state-aligned APT33 group (aka Peach Sandstorm, Elfin, MAGNALIUM, REFINED KITTEN, etc.) has modified their spear phishing tactics to target the human resources departments of predominantly Israeli and Israel-based companies with the group's signature FalseFront backdoor.	On the surface, FalseFront is a typical backdoor malware, written in .NET and capable of capturing screenshots, stealing credentials, and permitting remote access and control of a compromised machine. In this most recent campaign, APT33 has also been seen targeting an aerospace industry job application platform, likely to steal sensitive information. Somewhat atypically, stolen credentials are exfiltrated unencrypted over TCP, a curious oversight by normally skilled operators. In another sign of either a hurried development process or sloppy authorship, FalseFront's configuration data is both encoded and encrypted, but comments in the code remain, permitting simplified reverse engineering. Somewhat more typically, FalseFront also uses Signal as a command-and-control option, which is common among malicious actors attempting to both economize on development budgets and blend into seemingly normal traffic.[vii]
APT29 Deploying WINELOADER Malware Against EU Governments	The Russian state-aligned APT29 group recently carried out a targeted campaign against German political parties, likely ahead of the 2024 European Parliament elections, with the group's new WINELOADER backdoor malware.	The attack began with the typical spear phishing campaign, loading the group's EnvyScout/ROOTSAW implant, which, if successfully installed, would be used to deliver WINELOADER. The attacks began on or about 26 February, and interestingly, APT29 did not bother to change either the JavaScript obfuscation resource or the payload staging server. The former is understandable; the latter is the hallmark of a sloppy, poorly planned operation. Curiously, the codebase for WINELOADER is shared with two other previously embargoed APT29 backdoors, dubbed BURNTBATTER and MUSKYBEAT by Mandiant. The purpose of this operation is highly likely to be espionage rather than any attempt to ransom, interfere, or otherwise impact German government operations.[viii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Pyongyang Actors Targeting South Korean Semiconductor Firms	Beginning in December 2023, at least two South Korean semiconductor manufacturing companies have been targeted by North Korean state-aligned actors, according to the South Korean National Intelligence Service (NIS). The South Korean NIS provided no tactics, techniques, procedures, indicators of attack, or indicators of compromise. Both companies were compromised in December 2023, and one of these two companies was attacked again in February 2024, though South Korea's NIS declined to name the two companies targeted. One source reported that the attack targeted servers used to manage business documents, though this may have been a specific goal of the attackers rather than their sole point of entry. Given the huge number of vulnerabilities and zero days that came to light in December 2023, the North Korean attackers did not lack options. Once inside, the attackers utilized so-called live off the land tactics, using native tools and software available on the networks to conduct their malicious operations. Reportedly, the attackers managed to exfiltrate design plans, as well as plans for the fabrication facilities. The major gain from this attack for Pyongyang will likely be the ability to manufacture small semiconductor components for military and potentially commercial applications. Not only does Pyongyang not have access to the sub-20 nanometer stereolithographic semiconductor fabrication technology utilized worldwide, but such high-tech components are unsuitable for military applications anyway. A steady supply of low and mid-grade electronic components would do much to support North Korea's political aims. However, given the extent of economic sanctions it is unlikely to provide North Korea with an economic lifeline.[ix]
Kimsuky Actors Exploiting ScreenConnect Vulnerabilities to Load BABYSHARK Variant	During investigation of an attempted compromise at a client, Kroll's responder team identified a suspected variant of the North Korean Kimsuky group's flagship malware, BABYSHARK, being delivered at the end of an exploit chain consisting of two ConnectWise ScreenConnect vulnerabilities, CVE-2024-1709 and CVE-2024-1708. The setup wizard for ScreenConnect was exposed, allowing the attackers easy access to gain remote code execution ability. The malware itself is similar to BABYSHARK, a fully featured infostealer that gathers system info, hostnames, users, IP information, task lists, installed security software, and other information. Uniquely, the malware uses the native Windows certutil tool to create a PEM certificate from the collected data for exfiltration. This is a known hallmark of Kimsuky activity. One of the registry changes made by the attackers was to allow macros to run in Microsoft Office without notification; a curious change that is likely for post-compromise use or regaining access if the original implant is detected and remediated.[x]
Andariel Group Deploying New Malware with New Goals	A review of recent activity by the North Korean state-aligned Andariel Group has determined that the group is still conducting activities against domestic South Korean companies and has also added attacks for financial gain to their arsenal. ASEC researchers noted that while Andariel predominantly operates for espionage purposes and indeed still does target those entities in South Korea which are militarily, economically, and politically sensitive, the addition of attacks for financial gain is an interesting change. This suggests that Pyongyang may be having continued issues with funding their operations, as targeting of cryptocurrency exchanges and financial institutions was previously only conducted by APT37 (aka Reaper, Bluenoroff, etc.). The group also makes use of the MeshAgent remote access tool, ostensibly a legitimate remote administration tool being abused by the actors. DeepSeas notes that this tool is available on GitHub and would make for a good detection opportunity not just for Andariel activity but other actors utilizing remote administration software.[xi]

Earth Krahang Group Profits Off Simplistic Tactics	In a recent report by Trend Micro, the Chinese nation-state aligned Earth Krahang group's tactics were described in detail. Though the group has significant overlap with the well-known Earth Lusca group (aka MUSTANG PANDA), the two are likely different cells or teams. Unlike the relative technical sophistication of Earth Lusca, Earth Krahang makes use of the simplest tactics available to all actors, including spear phishing, brute-forcing of passwords, open-source scanning tools, and others. The group's targeting of governments and abusing the trust inherent between government officials is also unique. In one case, the attackers used a compromised email inbox to send nearly 800 spear phishing emails to the victim's address book. The group is known to continually harvest email addresses, credentials, and other data of use. Despite their relative simplicity, the group also maintains their own bespoke toolset. In addition to Cobalt Strike, the RESHELL and XDealer backdoors are used in the initial stages of Earth Krahang compromises; these have been in use since at least 2022, if not earlier, and remain under active development. Geographically, Earth Krahang's spread is worldwide. While the group predominantly operates in Southeast Asia, victims have been observed in Central Asia, the Middle East, North Africa, Europe, South America, Central America, and North America, demonstrating the scope and scale of the group's operations, most likely as a group providing initial access to other Chinese nation-state groups.[xii]
DEEP#GOSU Campaign Leaves a Deep Impact on South Korea	On 19 March 2024, the Securonix Threat Research team published information about a previously undisclosed attack campaign run by the North Korean APT group, Kimsuky. Securonix named the campaign “DEEP#GOSU.” After the victim opens a malicious .lnk file sent from Kimsuky through a phishing email, many steps are taken, with the end goal being to infect victims with TutRat, a remote access trojan (RAT) software that allows Kimsuky to enact full control over infected hosts. While TutRat is not novel and is typically easily blocked (due to it being loaded and executed into memory), it is able to avoid previously established antivirus protections. Along with using legitimate services - such as Dropbox or Google Docs - for C2 communication, it makes sense how this campaign could have flown under the radar. Kimsuky also employs the use of later stage scripts that allow the attackers to perform other malicious activities, such as monitoring the clipboard, keylogging, system enumeration, establishing persistence, and more.[xiii]
MuddyWater Group Modifies Phishing Emails to Target Israelis	Proofpoint has identified a recent spear phishing campaign by the Iranian state-aligned MuddyWater group (aka TA450, Mango Sandstorm, STATIC KITTEN) targeting Israeli employees at large multinational organizations. These employees are not necessarily employees of entirely Israeli companies either; meaning that employees belonging to organizations headquartered in North America, Europe, Asia, and other locales may be at risk. While the end goal of this campaign is to steal valid credentials, the attackers have changed up their tactics slightly. Rather than including a malicious link in the body of the spear phishing email, the links are now included in an attached PDF file. The attackers likely made this change to evade detection, as email attachment scanning is not ubiquitous. These links lead to various off-brand file hosting websites like Egnyte, OneHub, Sync, and TeraBox, retrieving a ZIP file with an MSI installer that loads AteraAgent - an ostensibly legitimate remote administration tool. Compromised email accounts are also used to send the spear phishing email, greatly complicating detection by the recipient and requiring software-based detections to catch.[xiv]

Dark Web Markets

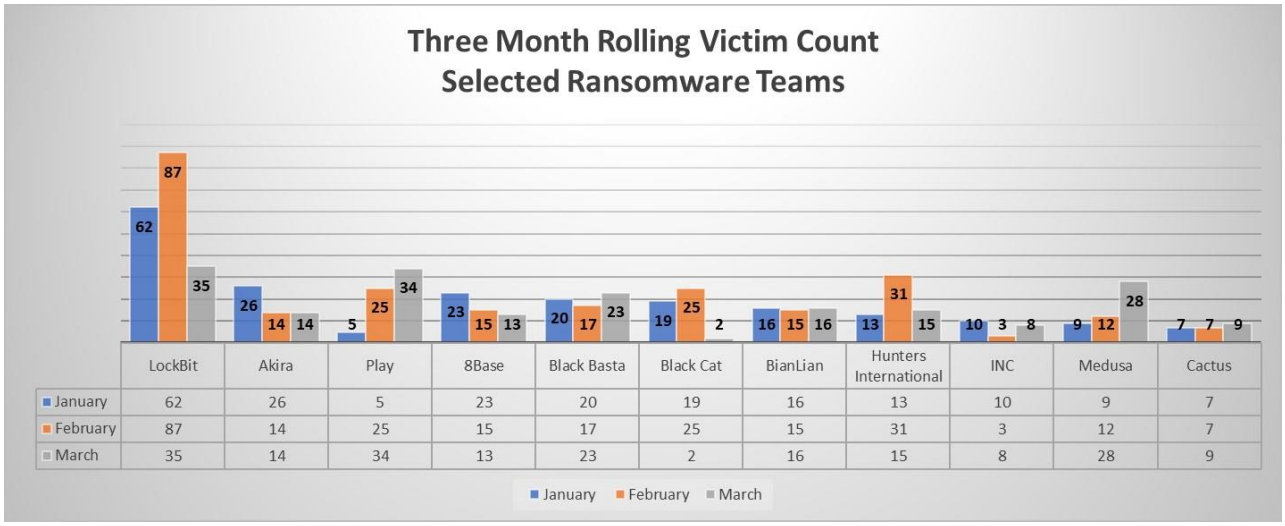
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

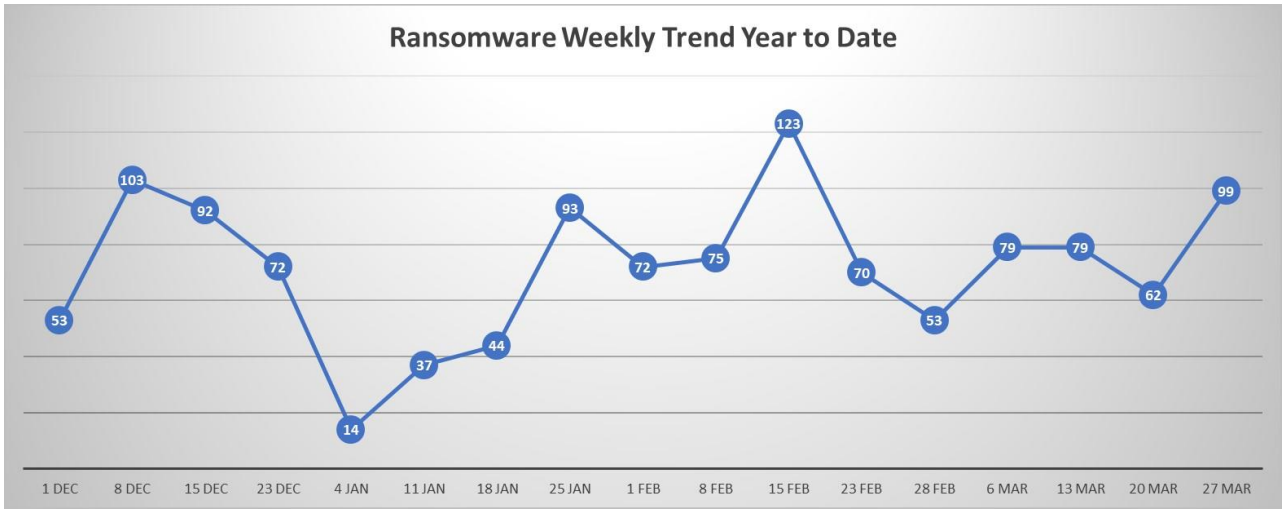
Activity	Note
Actor Developments	An affiliate of Black Cat submitted an arbitration request to a Russian-language crime forum claiming that he was entitled to the ransom payout of the Change Healthcare ransom – more than USD 20 million. The affiliate claimed that he still had 4 TB of information stolen from Change. Black Cat refused to pay and shut down the program in an apparent exit scam.
Access Sale	An actor on a popular Russian-language crime forum was selling RDP domain admin access to a South African air services company and an associated enterprise in the food service industry.
Access Sale	An actor on a popular Russian-language crime forum was selling access to an American automobile dealership with USD 2.4 billion in revenue for USD 8,000.
Access Sale	An actor on a popular Russian-language crime forum was selling RDP access to an unnamed American software security company with USD 51 million in revenue and specializing in the creation of security keys for IoT devices for USD 3,000. A known ransomware actor put in the buy now bid.
Access Sale	An actor on multiple popular crime forums was selling Fortinet access to an unnamed Indonesian enterprise in the aviation industry with USD 457 million in revenue for USD 800.
Tool Sale	An actor on a popular Russian-language crime forum is selling what he claims is a zero-day remote code escalation vulnerability in Microsoft Office. Notably he claims the vulnerability will trigger when opening MS Word or even when the cursor hovers over the icon or file name. Price is USD 200,000 payable in Bitcoin.
Access Sale	An actor on a popular Russian-language crime forum is selling RDP local admin access to a US pharmaceutical company with USD 511 million in revenue. He is also selling VPN domain user access to a US-based energy and utility company with USD 178 million in revenue.
Access Sale	An actor on a popular Russian-language crime forum was selling domain admin access to a US-based college with USD 257.7 million in revenue.
Access Sale	An actor on a popular Russian-language crime forum was selling RDWeb user domain access to a US-based pharmaceutical company with USD 60 million in revenue for USD 8,000.
Access Sale	An actor on a popular Russian-language crime forum was selling AnyDesk local admin access to a US-based customer relationship management software company with USD 52.5 million in revenue for USD 900.
Actor Developments	Recreational boat sales giant MarineMax filed an 8-K, reporting a "cybersecurity incident." MarineMax is listed as an "automobile dealer" with USD 2.4 billion in revenue on ZoomInfo. On 1 March, an actor on the XSS crime forum was noted selling access to a US-based automobile dealer with USD 2.4 billion in revenue. The actor shared a screenshot of the Horizon Cloud control panel and some of the desktops were named LAS-MMDesktop.
Actor Developments	LockBit ransomware posted the negotiation chat with San Diego based pharmaceutical company Crinetics. LockBit demanded USD 4 million from Crinetics, and Crinetics countered with USD 1.8 million, which LockBit walked away from.
Tool Sale	An actor on a popular Russian-language crime forum shared what he claimed was a proof of concept for an exploit targeting Microsoft Outlook CVE-2024-21378.

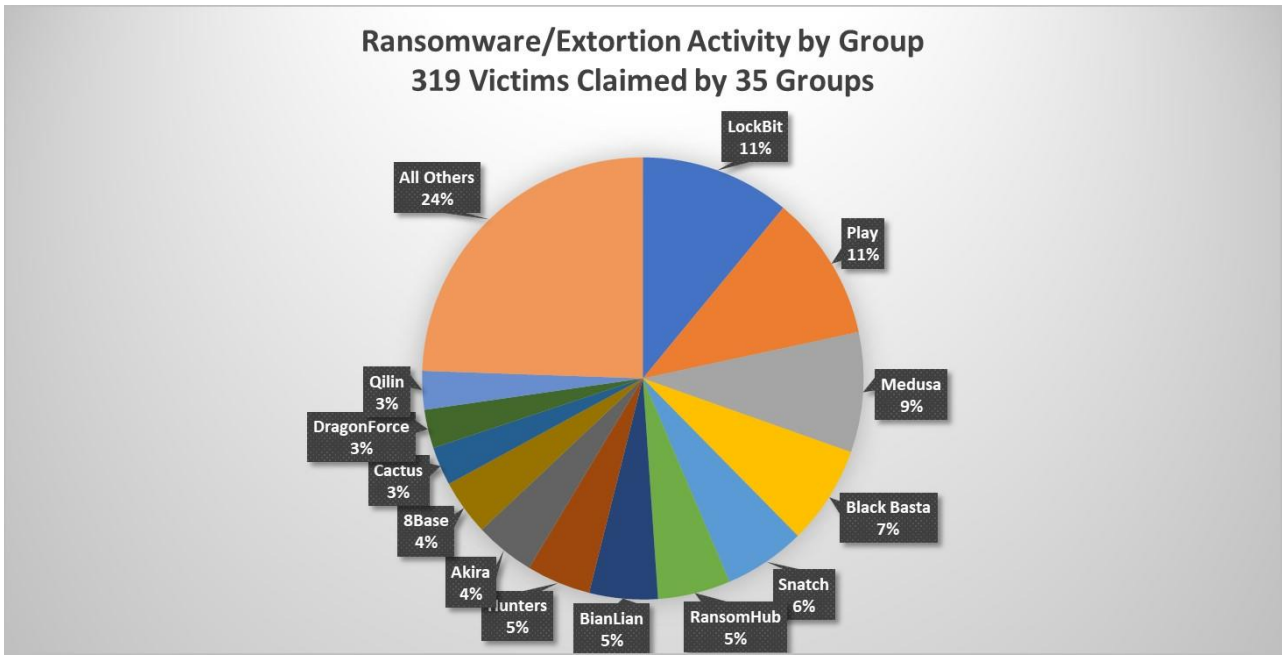
Access Sale	An actor on a popular Russian-language crime forum was selling what he claimed was admin access to an American company with USD 58.44 billion in revenue for USD 25,000. The access supposedly included access to the primary vSphere cluster controller, their AWS servers, and their Slack instance. There is no evidence that the access has been sold, and the actor did not provide any proof of access, leading other actors to express doubts about the validity of the offer.
Access Sale	An actor on a popular Russian-language crime forum was selling domain admin access to a Canadian industrial machinery company with USD 1.6 billion in revenue for USD 2,000.
Actor Developments	Fujitsu recently reported a data breach. In January 2024, an actor claimed to find almost 29,000 instances of companies using a particular remote command injection vulnerability in Cisco ASA 5500 series firewalls and made a demonstration video of himself allegedly obtaining a shell on Fujitsu systems using the vulnerability.
Access Sale	An actor on a popular Russian-language crime forum was selling full direct root access to the database of an Australian pizza chain with 89 restaurants. He claimed to upload a shell onto one sub-domain. There are at least three pizza chains with at least 89 restaurants in Australia.
Access Sale	An actor on a popular Russian-language crime forum was selling access to a U.S. state government court case portal with access to criminal case documentation and PII for the buy now price of USD 14,000.
Access Sale	An actor on a popular Russian-language crime forum was selling access to a Vietnamese airline with USD 60 million in revenue.
Actor Developments	Everest ransomware posted in multiple forums that they are specifically targeting law firms in the United States but will also consider Canadian and European law firms as well

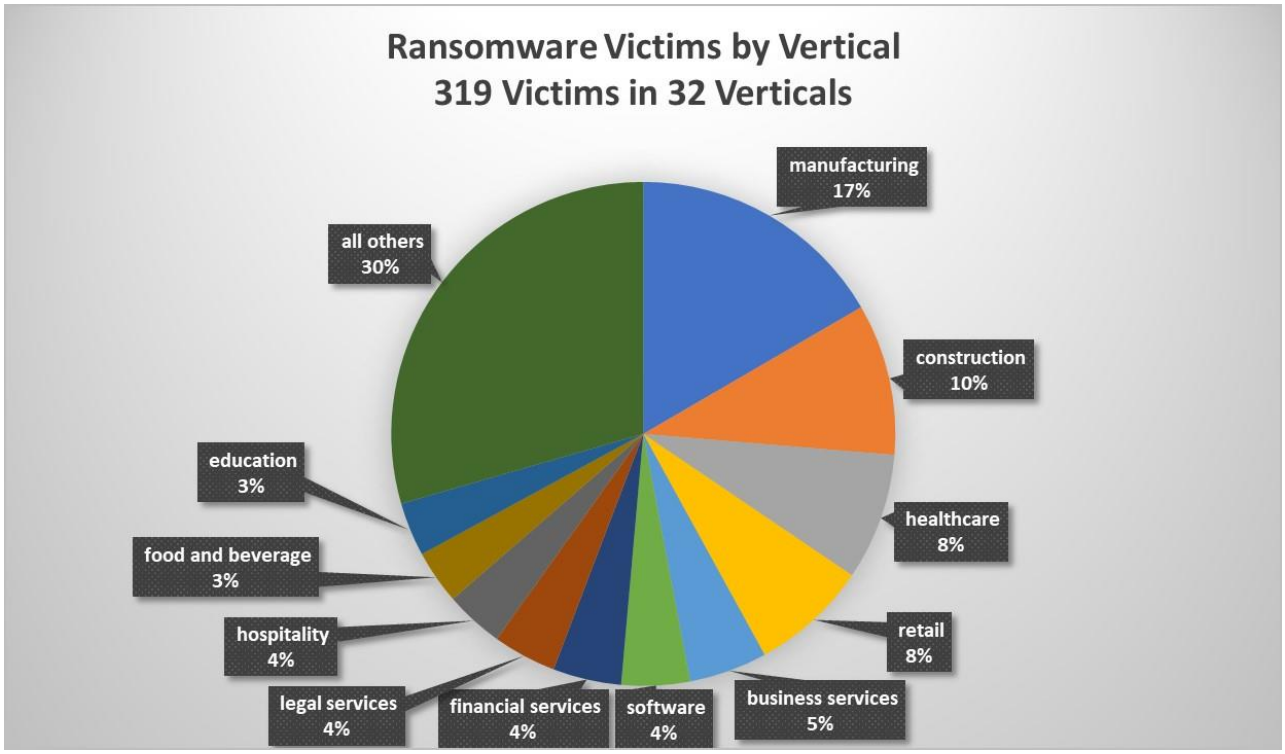
By The Numbers

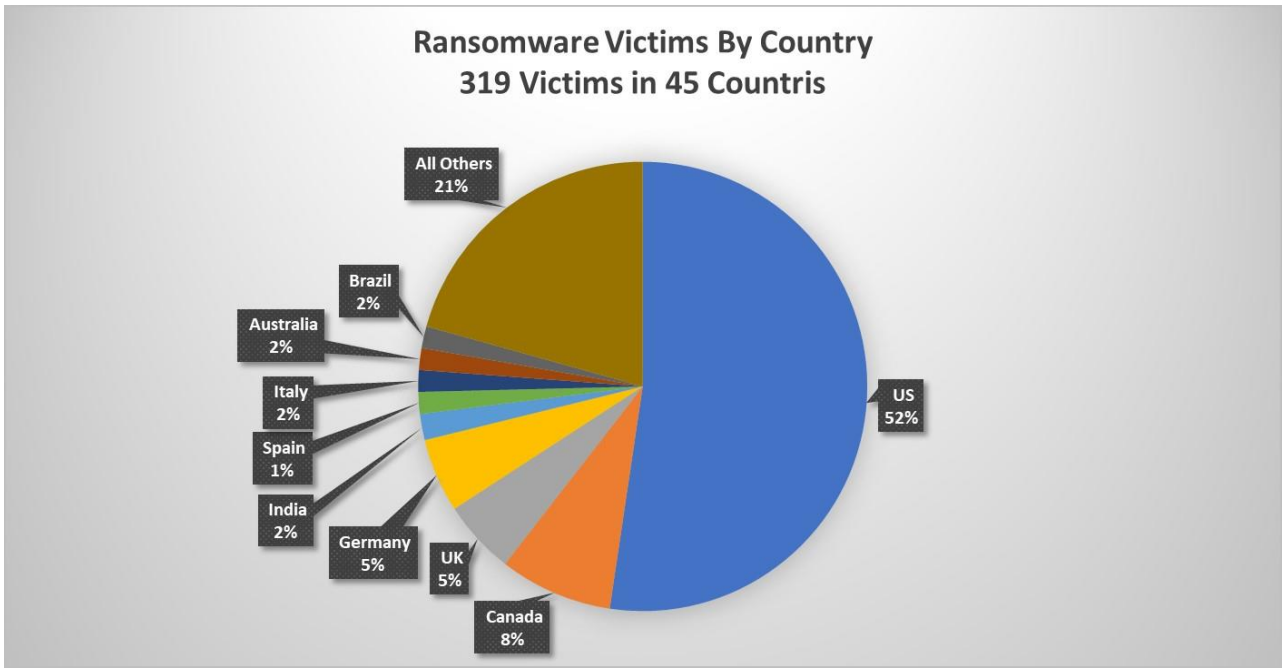
Summarizing incidents in graphical format






Ransomware/Extortion Activity by Group
319 Victims Claimed by 35 Groups
LockBit 11%
Play 11%
Medusa 9%
Black Basta 7%
Snatch 6%
RansomHub 5%
BianLian 5%
Hunters 5%
Akira 4%
8Base 4%
Cactus 3%
DragonForce 3%
Qilin 3%
All Others 24%


Ransomware Victims by Vertical
319 Victims in 32 Verticals
manufacturing 17%
construction 10%
healthcare 8%
retail 8%
business services 5%
software 4%
financial services 4%
legal services 4%
hospitality 4%
food and beverage 3%
education 3%
all others 30%


Ransomware Victims By Country
319 Victims in 45 Countris
All Others 21%
Brazil 2%
Australia 2%
Italy 2%
Spain 1%
India 2%
Germany 5%
UK 5%
Canada 8%
US 52%

New Detection Content

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

- CVE-2024-1403 OpenEdge Exploit
  - When the OpenEdge Authentication Gateway (OEAG) is configured with an OpenEdge Domain that uses the OS local authentication provider to grant user-id and password logins on operating platforms supported by active releases of OpenEdge, a vulnerability in the authentication routines may lead to unauthorized access on attempted logins. Similarly, when an AdminServer connection is made by OpenEdge Explorer (OEE) and OpenEdge Management (OEM), it also utilizes the OS local authentication provider on supported platforms to grant user-id and password logins that may also lead to unauthorized logins.

- OpenEdge Exploit
  - Looking for exploitation of CVE-2024-1403. Described as "When the OpenEdge Authentication Gateway (OEAG) is configured with an OpenEdge Domain that uses the OS local authentication provider to grant user-id and password logins on operating platforms supported by active releases of OpenEdge, a vulnerability in the authentication routines may lead to unauthorized access on attempted logins."

- AWS AMI Attribute Modification for Exfiltration
  - This search looks for suspicious AWS AMI attribute modifications, such as sharing it with another AWS account or making the full AMI image public. Adversaries are known to abuse these APIs to exfiltrate sensitive organization information stored in the AWS Resources. Thus, it is very important to monitor these seemingly benign API activities in CloudTrail logs.

- JetBrains TeamCity Authentication Bypass CVE-2024-2719
  - The CVE-2024-27198 vulnerability presents a critical security risk for JetBrains TeamCity on-premises servers, allowing attackers to bypass authentication and gain unauthorized access. This vulnerability can be exploited in several ways, each leading to the attacker gaining full control over the TeamCity server. One method of exploitation involves creating a new administrator user. An attacker can send a specially crafted POST request to the `/app/rest/users` REST API endpoint without authentication. This request includes the desired username, password, email, and roles for the new user, effectively granting them administrative privileges. Alternatively, an attacker can generate a new admin access token by targeting the `/app/rest/users/id:1/tokens` endpoint with a POST request. This method also does not require prior authentication and results in the creation of a token that grants administrative access. Both exploitation methods point to the severity of the CVE-2024-27198 vulnerability and highlight the importance of securing TeamCity servers against such threats. The manipulation of URI paths `/app/rest/users` and `/app/rest/users/id:1/tokens` through malicious requests enables attackers to gain unauthorized access and control, emphasizing the need for immediate remediation measures.

- Nginx ConnectWise ScreenConnect Authentication Bypass
  - This analytic detects attempts to exploit the ConnectWise ScreenConnect CVE-2024-1709 vulnerability, which allows an attacker to bypass authentication using an alternate path or channel. The vulnerability, identified as critical with a CVSS score of 10, enables unauthorized users to access the SetupWizard.aspx page on already-configured ScreenConnect instances, potentially leading to the creation of administrative users and remote code execution. The search query provided looks for web requests to the SetupWizard.aspx page that could indicate exploitation attempts. This detection is crucial for identifying and responding to active exploitation of this vulnerability in environments running affected versions of ScreenConnect (23.9.7 and prior). It is recommended to update to version 23.9.8 or above immediately to remediate the issue, as detailed in the ConnectWise security advisory and further analyzed by Huntress researchers.

[i] https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/
[ii] https://www.fortinet.com/blog/threat-research/vcurms-a-simple-and-functional-weapon
[iii] https://blog.sonicwall.com/en-us/2024/03/whitesnake-stealer-unveiling-the-latest-version-less-obfuscated-more-dangerous/
[iv] https://www.fortinet.com/blog/threat-research/banking-trojan-chavecloak-targets-brazil
[v] https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/, https://www.rapid7.com/blog/post/2024/03/04/etr-cve-2024-27198-and-cve-2024-27199-jetbrains-teamcity-multiple-authentication-bypass-vulnerabilities-fixed/
[vi] https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html
[vii] https://unit42.paloaltonetworks.com/curious-serpens-falsefont-backdoor/
[viii] https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties?linkId=9543905
[ix] https://www.reuters.com/world/asia-pacific/north-korea-broke-into-s-korean-chip-equipment-firms-seouls-spy-agency-says-2024-03-04/
[x] https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyshark
[xi] https://asec.ahnlab.com/ko/62771/
[xii] https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
[xiii] https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-deepgosu-attack-campaign/
[xiv] https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign