Monthly Threat Intelligence Rollup

DEEP seas

01/01/24-01/31/24

Notable Cyber Attacks

Summary of noteworthy cyber attacks in the last thirty days.

Incident	Activity Summary
Ukrainian Telecommunications Provider KyivStar Destroyed in Cyberattack	A recent cyberattack by the presumed Russian Solntsepek hacktivist group has been confirmed to have seriously damaged the Ukrainian telecommunications operator KyivStar's networks. This attack was later attributed to the actions of the Russian state-aligned Sandworm team. According to post-incident analysis, the attackers were present in KyivStar's networks since at least May 2023, though they had gained full access only in November 2022. The attack effectively cored out the heart of KyivStar's networks, destroying thousands of virtual computers, servers, and other infrastructure. Evidence was found of repeated attempts to follow up on the December attack, pointing towards a desire to both destroy and suppress KyivStar for as long as possible. Though Ukrainian authorities stated that no military communications were being routed through KyivStar's networks, and further attacks were unsuccessful. DeepSeas believes that the focus on disabling telecommunications networks is part of an attempt to silence networks of so-called 'partisans' in Ukraine who are reporting Russian troop and armor movements to Ukrainian authorities, as well as cause additional chaos and panic. More worrying is the operational experience gained by Russian hacking teams in compromising these entities, experience which may be useful in other conflicts.[i]
Attacks on Danish Critical Infrastructure Not Entirely the Work of The Sandworm Group	Continued analysis of a widespread attack against Danish energy companies has revealed further details downplaying the role of the Russian state-aligned Sandworm Group. Forescout researchers following up on the incident noted that the attacks were actually two separate campaigns. The first campaign was linked to Sandworm Group based on old or outdated indicators, which lowers the confidence of attribution significantly.The second campaign appeared to have been part of a larger, less targeted campaign by unrelated threat actors. Other companies in addition to the Danish energy companies were affected as well, reducing confidence that the attacks were targeted and heightening confidence that a cybercriminal group, possibly a ransomware actor, was responsible for the mass exploitation.[ii]
TeamViewer Logins Used by Criminals to Deliver Ransomware	Security company Huntress has recently observed a spate of attempts by unknown threat actors seeking to abuse valid login credentials for existing and legacy TeamViewer installations for the purposes of delivering ransomware. The scope and scale of these attacks is currently unknown, though Huntress did note that the attackers were delivering ransomware built using a leaked version of the LockBit ransomware group's builder for LockBit Black ransomware. In the cases observed by Huntress, the attackers did not attempt to move laterally or conduct post-compromise exploitation. Furthermore, the attackers were stymied by endpoint security, as their knockoff ransomware was prevented from executing properly. Other samples identified by DeepSeas analysts in VirusTotal agree with the findings by Huntress, specifically that the ransomware binary is identified as LockBit 3, though with a non-standard ransom note.[iii]
ESET Does Its Part in Disrupting Grandoreiro	In a collaboration with the Federal Police of Brazil, ESET researchers continue to try to push back against the Grandoreiro botnet in a long-term tracking operation against the people behind it. Grandoreiro is a banking trojan from Latin America that has been active since 2017. The malware works by periodically checking the foreground window to find a running web browser. After finding one, along with the browser's name, it matches any string from a hardcoded list of bank-related strings. The malware then initiates communication with its C&C server, sending requests at least once a second until terminated. Through their research, ESET found that the domain generation algorithm (DGA) Grandoreiro has used since around October 2020 is the only way Grandoreiro knows how to report to a C2 server. It produces one main domain, and optionally several failsafe domains, per day. Besides the current date, the DGA accepts static configuration as well, and they have observed 105 such configurations as of their blog post.[iv]

Stately Taurus Attacks Myanmar Ministry of Defense Amid Ongoing Border Conflicts	After multiple attacks by Three Brotherhood Alliance (3BHA), a rebel alliance currently in control of Myanmar, China has expressed worry about the impact of these attacks on the trade routes along the Myanmar-China border. During this time of stress for the nations, CSIRT-CTI has found evidence of cyber attacks specifically directed at the Myanmar Ministry of Defense, aligning with the ongoing situation in the country. Given their past tactics, techniques, and procedures (TTPs) resemble this case, CSIRT-CTI believes it is highly probable that Stately Taurus, one of the most active Chinese APT groups, is responsible for these attacks. The most prominent of these TTPs is their use of legitimate software, such as a binary developed by engineering firm Bernecker & Rainer (B&R), along with a component of the Windows 10 upgrade assistant to sideload malicious Dynamic-Link Libraries (DLLs). Moreover, a significant number of campaigns attributed to this threat actor have been reported to disguise network traffic by making it appear to be related to Microsoft update traffic. Stately Taurus operations are known to coincide with the geopolitical interests of the Chinese government, including previous cyber espionage activities against Myanmar. Since this group targets not only Asian nations but also European and North American countries, it is advisable to implement countermeasures to protect against potential attacks from this group.[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
Ivanti Locks Down Access to Advisory on Recent CVE	After a rough July and August 2023, software management company Ivanti has reportedly fixed a new remote code injection vulnerability in Ivanti Endpoint Management (EPM) software that permits attackers the ability to gain control of enrolled devices or the EPM server itself.	CVE-2023-39336 is rated critical at 9.6 severity and affects versions of Ivanti EPM 2021 and EPM 2022 prior to Service Update 5. Installing Service Updated 5 resolves the issue. More worrying is that Ivanti has locked down public access to their detailed technical advisory for CVE-2023-39336, complicating the work of network defenders attempting to learn more about the exploit. While this does provide a modicum of security by preventing malicious actors from accessing the same information, the lack of public technical information remains a problem for network defenders. Fortunately, Ivanti has stated that there is no evidence that CVE-2023-39336 has been exploited in the wild, though this falls firmly on the side of "trust but verify" as not all software vendors are as forthright as others are regarding vulnerabilities in their products.[vi]
UNC4990 Dusts Off Old Tactic Using New Malware	Mandiant Managed Defense has been monitoring the activities of UNC4990, an actor with a particular focus on targeting users in Italy for financial gain.	UNC4990, which Mandiant believes has been active since at least 2020, have been seen employing what can be considered a less effective method of malware delivery, weaponizing USB drives. Despite this, UNC4990 shows continuous growth in its tools, tactics, and procedures (TTPs), which allow it to steal from new victims. They have done this using both a custom downloader they have named EMPTYSPACE (also known as VETTA Loader or BrokerLoader), and QUIETBOARD, a Python based, multifaceted backdoor capable of many different malicious actions, including arbitrary command execution, clipboard content manipulation for crypto currency theft, USB/removable drive infection, screenshotting, system information gathering, and C2 communication. Additionally, the backdoor has the capability of modular expansion and running independent Python based code/modules. They manage to run this backdoor by exploiting legitimate services; however they do so without exploiting any vulnerabilities or misconfigurations, ensuring the hosted content poses no direct risk to everyday users, allowing for a stealthy intrusion. It is also worth noting that UNC4990 has transitioned from using what seems like harmless encoded text files to hosting malicious payloads on popular websites like Ars Technica, GitHub, GitLab, and Vimeo, showing their increase in sophistication. The use of USB drives is also a curious and difficult tactic to scale up. While USB drives can be had from any number of retailers at low cost, especially those small in size, the infrastructure required to distribute these USB drives makes this tactic uneconomical for widespread campaigns.[vii]
Jenkins Security Flaw Leads to Critical Vulnerability	Sonar's Vulnerability Research Team has discovered multiple new security vulnerabilities in Jenkins, a well-known, open-source Continuous Integration and	Since Jenkins had a market share of around 44% in 2023, its popularity is clearly self-stated, which means that the potential impact of any security vulnerabilities in Jenkins is large. In this case, the first of the discovered critical vulnerabilities, CVE-2024-23897, allows unauthenticated attackers to read a limited amount of arbitrary files' data, and attackers with "read-only" permissions were authorized to an entire arbitrary file from a

	Continuous Deployment (CI/CD) software, used for developers to automate the various aspects of the software development lifecycle, such as the building, testing, and deployment stages.	Jenkins server. Attackers could then leverage this vulnerability by reading Jenkins secrets, escalating their privileges and eventually execute arbitrary code on the server. The second discovered vulnerability is also of high severity and is a cross-site WebSocket hijacking (CSWSH) vulnerability tracked as CVE-2024-23898, which allows an attacker to execute arbitrary CLI commands by manipulating a victim to click on a link. Both of these vulnerabilities were thankfully patched in Jenkins versions 2.442 and LTS 2.426.3, so any Jenkins servers currently active should be inspected and made sure they are upto-date to avoid these vulnerabilities. DeepSeas recommends patching immediately, as Jenkins servers are often targeted first by crypto mining malware for their high processing power.[viii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Two Ivanti Zero Days Exploited by Chinese Nation-State Actors	Beleaguered Ivanti has reportedly fixed two new zero-day exploits in their flagship enterprise VPN solution, Ivanti Connect Secure (ICS). Reporting by Volexity suggests that Chinese state-aligned actors have been exploiting these zero-days in targeted attacks against at least 10 unnamed victims. The vulnerabilities in Ivanti ICS (formerly known as Pulse Secure Connect) CVE-2023-846805 and CVE-2024-21887, an authentication bypass and remote command Injection vulnerability respectively, are both moderate to high severity, though when chained together they have proven to be devastatingly effective. Together, two zero days provide the attackers with the ability to steal login credentials and a trivial route to access the rest of their targets' networks. At present, over 15,000 Ivanti ICS installations are publicly accessible worldwide, particularly in the U.S., Japan, Germany, France, and Canada. The attackers were observed by Volexity loading webshells (GLASSDOOR) and tools (ReGeorg) on multiple internal and external-facing web servers, and incident responders noted that the attackers had wiped the Ivanti ICS logs. Neither of these are hallmarks of purely nation-state activity, though the destruction of logs will likely provide an excellent detection opportunity in addition to those provided by Volexity and other security companies.[ix]
Mint Sandstorm Targeting Research Organizations in Europe	The Iranian state-aligned Mint Sandstorm group has recently been observed by Microsoft researchers conducting a highly targeted spear phishing campaign against researchers, journalists, and academics at universities and think tanks across Europe, particularly those specializing in Gazan and Middle Eastern affairs. The attackers were noted spending time preparing a rapport with their targets, conversing and sending benign and harmless documents before finally sending a weaponized payload. The payload observed is previously unseen, consisting of the MischiefTut or MediaPl backdoors. MischiefTut is a custom PowerShell-based backdoor that acts as a bridgehead for secondary payloads, while MediaP1 maintains the same functions but instead masquerades as Windows Media Player.[x]
Russian COLDRIVER Group Widens Targeting Across Western Europe	The Russian state-aligned COLDRIVER threat actor group, more commonly known as Callisto and overlapping with the Gamaredon group, has been identified widening their net of phishing activity away from solely against Ukraine to include high profile individuals in NGOs, former intelligence and military officers, and NATO governments across Western Europe. Similar to the Iranian state-aligned Mint Sandstorm group, COLDRIVER has been observed building rapport with targets before sending them a PDF file weaponized with the group's only known bespoke malware, the SPICA backdoor. This backdoor is a fully featured backdoor written in Rust and capable of conducting reconnaissance on a compromised system.[xi]
Blackwood Group Hijacking Application Updates	A recent ESET report details activities of a poorly documented Chinese state-aligned group dubbed Blackwood, which has been observed engaging in cyber espionage activities against Chinese, Japanese, and United Kingdom targets since at least 2018. The group utilizes a unique method of malware delivery; the group's NSPX30 implant is delivered via so-called adversary-in-the-middle (AitM) attacks via legitimate software updates, which are also used to route command-and-control (C2) traffic to avoid detection. Analysis by ESET determined that the underlying codebase of the NSPX30 malware dates to 2005, and the first rough version of NSPX30 to 2008, built upon this dated codebase. Timestomping was determined to not be a factor in the analysis, making NSPX30 one of the oldest malware lineages known. Variants were observed in attacks in 2011, 2014, 2016, and finally in the first variant of NSPX30 in 2018. The use of legitimate software updates to deliver the malware is a tactic strikingly like the compromises of software such as CCleaner in 2017, though the implant itself appears to be a second-stage payload intended for long-term monitoring of systems and individuals of interest. In the case of the victim from the United Kingdom, the NSPX30

	malware was configured to intercept and exfiltrate chat client messages for Tencent QQ.[xii]
Nation-State Actors Exploiting VMware Vulnerability for Nearly Two Years	Though VMware patched an out of bounds write vulnerability (CVE-2023-34048) in VMware vCenter in October 2023, Mandiant researchers have determined that the vulnerability had been under active and long-term exploitation by a Chinese state-aligned actor, UNC3886, since at least late 2021 if not longer. Further compromises were observed in 2022 and continued until 2023, when the vulnerability was finally detected and patched. The attackers removed the vmdird core dumps as well to cover their tracks and utilized multiple Python-based backdoors in the VIRTUALPIE and VIRTUALPITA. Once established, the attackers then utilized CVE-2023-20867 to harvest credentials, access other guest virtual machines, and collect/exfiltrate files from targeted VMs. Analysis of the UNC3886 actors' previous activities determined that the actors responsible prefer targets in the defense industrial base, government, telecommunications, and high technology sectors, predominantly in the Asia-Pacific region as well as the United States, indicating that the group is focused on espionage rather than cybercrime.[xiii]
APT29 Launches Espionage Spree, Targeting HPE, Other Tech Companies	On 19 January 2024, Hewlett Packard Enterprise Company (HPE) filed a declaration with the Securities Exchange Commission (SEC) that in December, HPE discovered Russian SVR threat actors (APT29) had accessed and exfiltrated data from HPE mailboxes in HPE's cloud-based email environment. Additionally, on 12 January 2024, Microsoft reported that APT29 threat actors compromised a publicly exposed test account, which Russian SVR then used to compromise Microsoft corporate email accounts. Further analysis of the attack determined that HPE had been compromised previously in 2023, and the attack was not properly remediated, leading to a second compromise. The root of the problem lay in Microsoft's implementation of OAuth, with the attackers taking advantage of the test account, which was poorly managed, permitting APT29 to access the inboxes of not just HPE but numerous other companies in the United States and Europe, including IT service providers, NGOs, software developers, and government organizations. The inboxes of these organizations' leadership were of particular interest, with Russian actors likely intent on finding details regarding developments aimed at either isolating Russia or intelligence pertaining to these organizations' efforts to counter Russian cyber espionage and cyber criminal activities. This is concurrent with the Iranian nation state-linked Mint Sandstorm actors' efforts to carry out cyber espionage activities against similar target sets with intent to gather intelligence on developments in the Middle East.[xiv]
Volt Typhoon Puts SOHO Routers in the Eye of the Storm	In a dual report made by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), the two U.S.-based government agencies warn of Volt Typhoon, a People's Republic of China (PRC) state-sponsored actor who has been active since at least 2021. They have been known to typically focus on espionage and information gathering and have been seen targeting critical infrastructure organizations in the U.S. and Guam in the past. In this case, Volt Typhoon has been seen targeting small office/home office (SOHO) routers, compromising them using vulnerabilities in the router's software. The threat actor's goal with these routers is to use them as a launch pad for furthering their objective of targeting critical infrastructure. In response to this, CISA and the FBI released three principles that they believe these router manufacturers should follow. The first principle, "Take Ownership of Customer Security Outcomes," goes over methods of securing routers, such as changing default credentials and the like. The second principle, "Embrace Radical Transparency and Accountability," means that manufacturers should be open and honest about any discovered vulnerabilities and disclose them to the CVE program. And finally, the third principle, "Build Organizational Structure and Leadership to Achieve These Goals," states the manufacturers should face be held more responsible for the security of their products, and that it should not be the burden of customers, the economy, or our national security.[xv]

Dark Web Markets

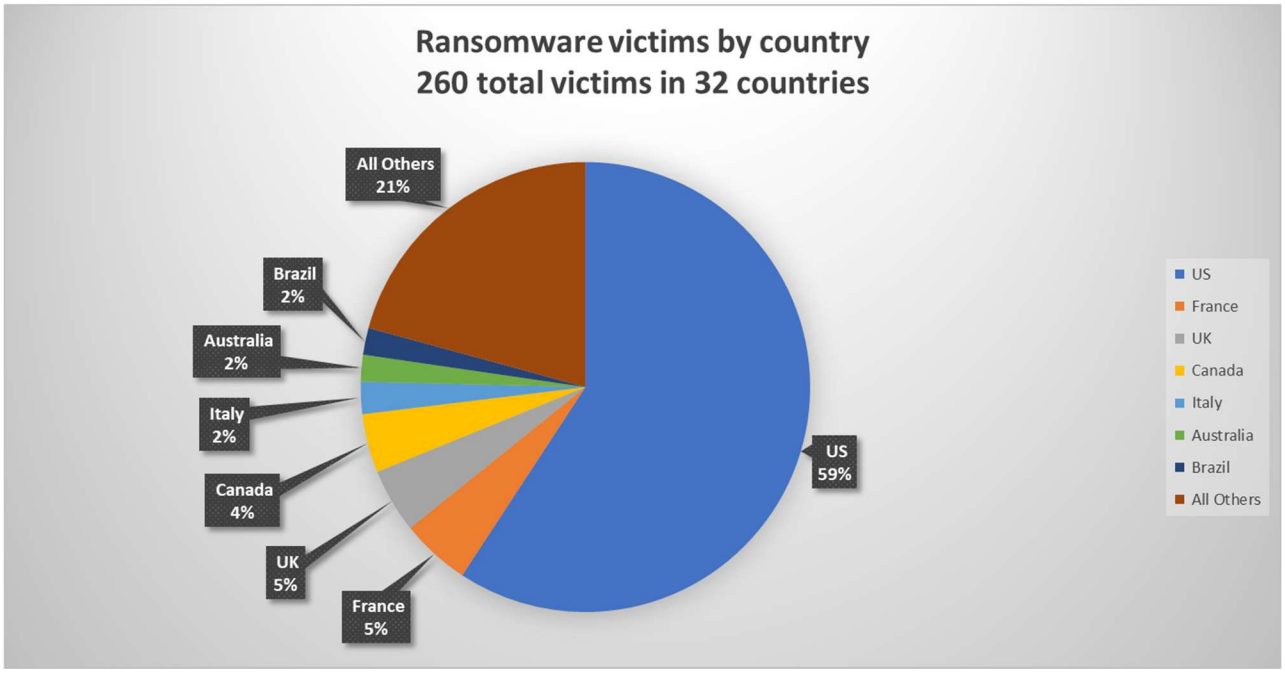
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

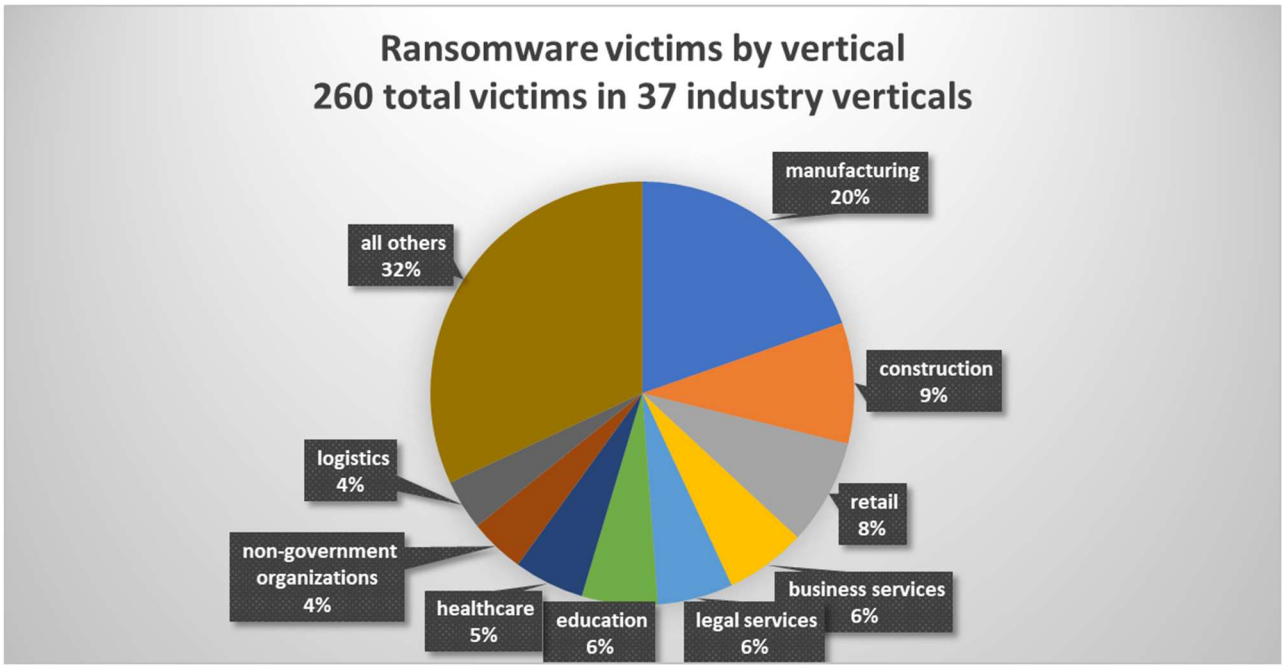
Activity	Note
Access Sale	An actor on a Russian-language crime forum was selling Citrix access to a company in the energy, utilities, and waste vertical with USD 84.4 million in revenue.
Access Sale	An actor on a Russian-language crime forum was selling RDP domain admin access to a Chinese manufacturer with USD 32.1 billion in revenue.
Tool Sale	An actor on a Russian-language crime forum was noted selling what he claimed is a remote command injection vulnerability in Cisco ASA 5500 series firewalls for USD 1 million. He claimed there are 6,317 companies vulnerable to this flaw. He did not offer a more detailed description of the vulnerability, and, as he is a new user, his credibility is unknown.
Access Sale	An actor on a Russian-language crime forum was selling access to what he claimed is a control panel allowing real time viewing and controlling of ships and cargos on the Danube River for USD 50,000.
Access Sale	An actor on a Russian-language crime forum with only one post was selling access to what he claimed was the Central IT Center of Poland, noting that for the people who know it is the route to Polish servers. He claimed that "government software, encryption systems, bank card accounting systems, VPNs, TeamViewers, and much else" is stored there. He provided several screenshots purporting to demonstrate access. He is a new user, and his credibility is unknown.
Access Sale	An actor on a Russian-language crime forum is selling Citrix access to a Norwegian company in the marine shipping and transportation vertical with USD 1.1 billion in revenue for a buy now price of USD 5,000.
Access Sale	An actor on a Russian-language crime forum is selling access to the Saudi Municipality of Holy Mecca for USD 10,000. He described it as "a rich government resource."
Tool Sale	An actor on a Russian-language crime forum is selling what he calls a remote code execution exploit in an unnamed popular IoT product with more than 100,000 hits on Shodan and Fofa for USD 25,000. He did not further describe the exploit.
Access Sale	An actor on a Russian-language crime forum is selling local admin access to a U.S. based home accessories and home furniture manufacturer/retailer with USD 153 million in revenue for USD 4,000. He posted a screenshot purporting to show access.
Access Sale	An actor on a Russian-language crime forum and an English-speaking crime forum was selling FTP access to McDonald's, including private source code from McDonalds' GitHub repository and employee and banking data.
Access Sale	An actor on a Russian-language crime forum was selling Citrix admin access to a U.S. based airline with more than USD 500 million in revenue.
Access Sale	An actor on a Russian-language crime forum was selling access to a police emergency data request panel for USD 5,000, offering illicit access to multiple law enforcement databases and giveing a malicious actor the ability to issue a fraudulent emergency law enforcement request to enterprises.
Access Sale	An actor on a Russian-language crime forum was selling RDP domain admin access to U.S.-based defense contractor Moog (NYSE: MOG.A) for USD 19,000.
Access Sale	An actor on a Russian-language crime forum was selling Office 365 passwords and session cookies for employees of the District of Columbia for USD 200.

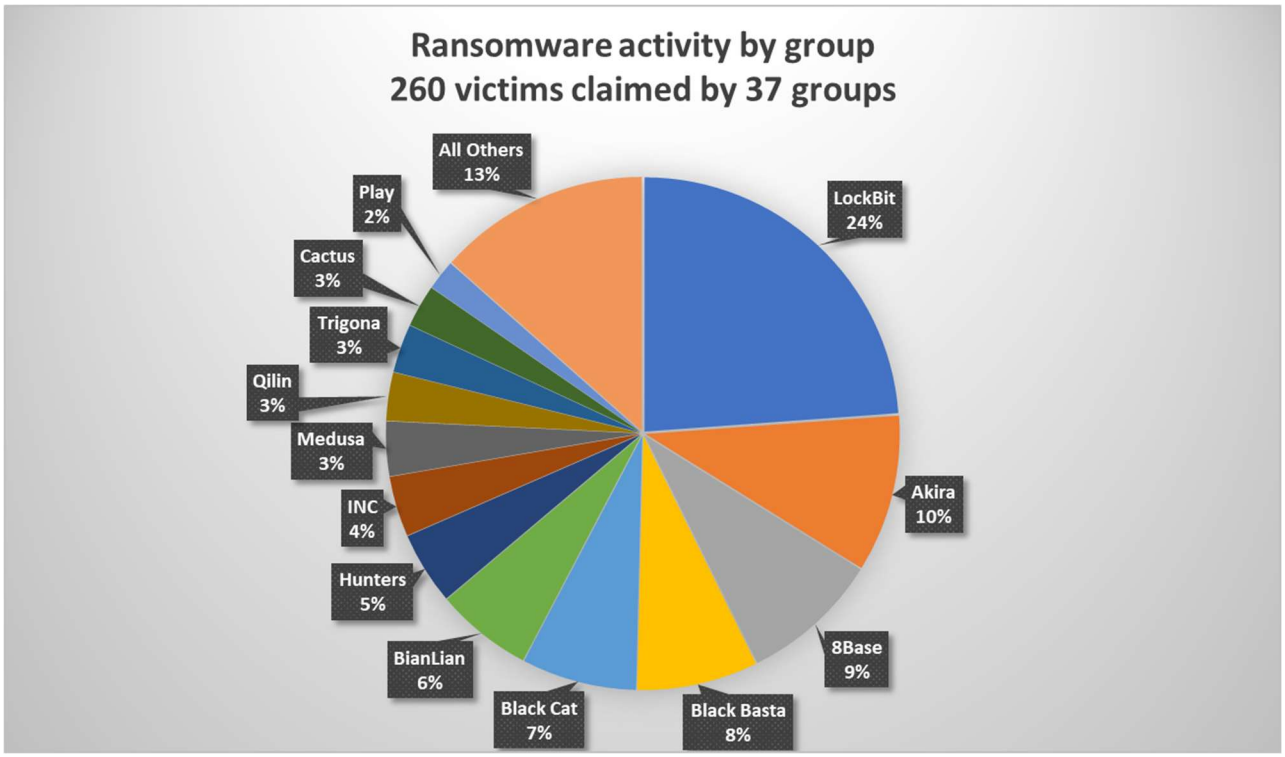
Access Sale	An actor on a Russian-language crime forum actor was selling 4 TB of files from UK based advertising consultancy 8th Day Strategy. The files included information belonging to clients such as Bayer, Apple, Amazon, Diageo, Chanel, Unilever, AXA, L'Oreal, Adidas, and General Mills. Asking price is USD 50,000.
Access Sale	An actor on an English-language crime forum was selling what he claimed was data stolen from the Texas State Comptroller Office.
Actor Developments	Russian security company AN-Security was attacked by someone using LockBit ransomware. The consensus in the Russian-language XSS forum was that this wasn't an official LockBit affiliate that carried out the attack. Today, LockBit accused a veteran member of the Exploit crime forum of not only being the head of Cl0p ransomware, but also of carrying out the attack on the Russian company to damage LockBit's reputation. LockBit put out a bounty for information about Signature's identity. Another actor in the XSS forum accused Signature of having lost all his money back when he was working for Revil ransomware to drugs and/or gambling. On 22 Jan, a user attempted to sell the AN-Security data on Breach Forums for 100 bitcoin. A well-known Russian crime forum actor, Bratva, responded to the Breach Forums post by denying that LockBit had anything to do with this attack on a Russian company.
Access Sale	An actor on a Russian-language crime forum was selling RDP domain admin access to a stock exchange listed, Singapore based consumer electronics and computer retailer with 800 employees and USD 900 million in revenue for a buy now price of USD 2,000.
Access Sale	An actor on a Russian-language crime forum was selling access to a POS terminal located in Kentucky.
Access Sale	A new access seller on a Russian-language crime forum, whose credibility cannot be judged because of his lack of history, was selling Fortinet access to a U.S. based technology company with more than USD 4 billion in revenue for a buy now price of USD 10,000. The access has been on sale since 23 Jan and was originally priced at USD 15,000. There is likely a reluctance to engage with the actor in the community because of his newness and lack of vendor deposit.

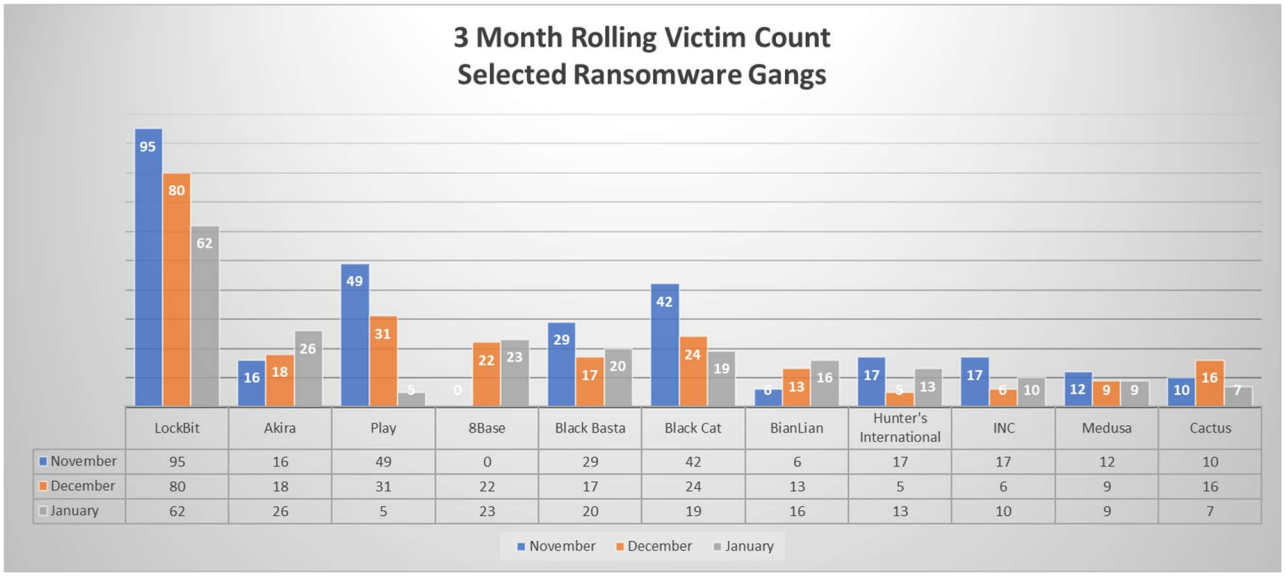
By The Numbers

Summarizing incidents in graphical format

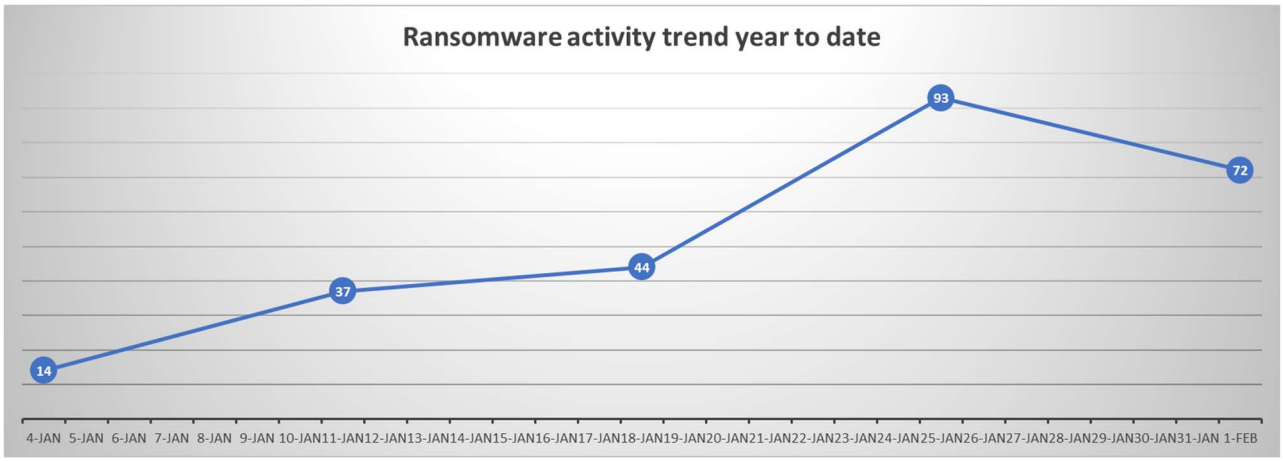








	LockBit	Akira	Play	8Base	Black Basta	Black Cat	BianLian	Hunter's International	INC	Medusa	Cactus
November	95	16	49	0	29	42	6	17	17	12	10
December	80	18	31	22	17	24	13	5	6	9	16
January	62	26	5	23	20	19	16	13	10	9	7


Ransomware activity trend year to date
14
37
44
93
72
4-JAN 5-JAN 6-JAN 7-JAN 8-JAN 9-JAN 10-JAN 11-JAN 12-JAN 13-JAN 14-JAN 15-JAN 16-JAN 17-JAN 18-JAN 19-JAN 20-JAN 21-JAN 22-JAN 23-JAN 24-JAN 25-JAN 26-JAN 27-JAN 28-JAN 29-JAN 30-JAN 31-JAN 1-FEB

New Detection Content

Noteworthy new detection logic added in the last 30 days, excluding rule tuning. The following is a sampling of rules created by DeepSeas out of 1,216 created.

- SharpKatz Credential Stealing Tool
  - This detection is looking for the SharpKatz tool, which is a variant of Mimikatz.https://github.com/b4rtik/SharpKatz

- PsExec Spawning CMD or PowerShell | PsExec Service Execution | Renamed PsExec Service
  - These detections are looking for PsExec commands. PsExec is a tool that can used to execute remote commands and is used by threat actors and system administrators. The presence of PsExec should be verified if allowed in a customer environment, and the process commands should be investigated for maliciousness.
  - https://thedfirreport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/
  - https://attack.mitre.org/software/S0029/

- Scheduled Task Command Using Rundll32 for Persistence
  - This detection is looking for the process schtasks.exe with a command line containing rundll32.exe. This was seen used as a persistence and execution mechanism during the TeamCity Intrusion saga in the references. Here is the malicious example from that intrusion:
    - schtasks.exe /create /SC ONLOGON /tn "\Microsoft\Windows\DefenderUPDService" /tr "\"C:\Windows\system32\rundll32.exe\" \"C:\Windows\system32\AclNumsInvertHost.dll\",AclNumsInvertHost"
  - https://www.fortinet.com/blog/threat-research/teamcity-intrusion-saga-apt29-suspected-exploiting-cve-2023-42793
  - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

- Renamed LogMeIn Remote Access Software | Renamed AnyDesk Remote Access Software
  - These detections are looking for a renamed remote access software process. These can give an attacker remote access to a host for command and control. A renamed one is highly suspicious and should be verified if allowed in the environment.
  - https://attack.mitre.org/techniques/T1219/

- Windows System User Privilege Discovery
  - This analytic looks for the execution of `whoami.exe` with /priv parameter. This whoami command is used to display or show the privileges assigned to the current user account. This hunting query can be a good pivot start to look for suspicious usage of whoami application that might be related to a malware or adversaries.

- Windows Known GraphicalProton Loaded Modules
  - The following analytic identifies a potential suspicious process loading DLL modules related to Graphicalproton backdoor implant of SVR. These DLL modules have been observed in SVR attacks, commonly used to install backdoors on targeted hosts. This anomaly detection highlights the need for thorough investigation and immediate mitigation measures to safeguard the network against potential breaches.

- GitHub Two-Factor Authentication Disable
  - Two-factor authentication is a process where a user is prompted for an additional form of identification during the sign-in process, such as to enter a code on their cellphone or provide a fingerprint scan. Two-factor authentication reduces the risk of account takeover. Attackers will want to disable such security tools in order to go undetected.

- Lateral Movement via DCOM
  - This query detects a fairly uncommon attack technique using the Windows Distributed

Component Object Model (DCOM) to make a remote execution call to another computer system and gain lateral movement throughout the network.

- Ref: http://thenegative.zone/incident%20response/2017/02/04/MMC20.Application-Lateral-Movement-Analysis.html'

[i] https://ssu.gov.ua/novyny/sbu-dopomohla-vidbyty-novi-kiberataky-rf-na-kyivstar-illia-vitiuk
[ii] https://cyberscoop.com/sandworm-sektorcert-critical-infrastructure-zyxel/
[iii] https://www.huntress.com/blog/ransomware-deployment-attempts-via-teamviewer
[iv] https://www.welivesecurity.com/en/eset-research/eset-takes-part-global-operation-disrupt-grandoreiro-banking-trojan/
[v] https://csirt-cti.net/2024/01/23/stately-taurus-targets-myanmar/
[vi] https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336, https://www.bleepingcomputer.com/news/security/ivanti-warns-critical-epm-bug-lets-hackers-hijack-enrolled-devices/
[vii] https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware
[viii] https://www.sonarsource.com/blog/excessive-expansion-uncovering-critical-security-vulnerabilities-in-jenkins/
[ix] https://arstechnica.com/security/2024/01/actively-exploited-0-days-in-ivanti-vpn-are-letting-hackers-backdoor-networks/, https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
[x] https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
[xi] https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/
[xii] https://www.welivesecurity.com/en/eset-research/nspx30-sophisticated-aitm-enabled-implant-evolving-since-2005/
[xiii] https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021
[xiv] https://www.sec.gov/Archives/edgar/data/1645590/000164559024000009/hpe-20240119.htm
[xv] https://www.ic3.gov/Media/News/2024/240131.pdf