



Publish date: March 28, 2024

Global Cyber Threat Intelligence (CTI)

Annual Cyber Threat Trends

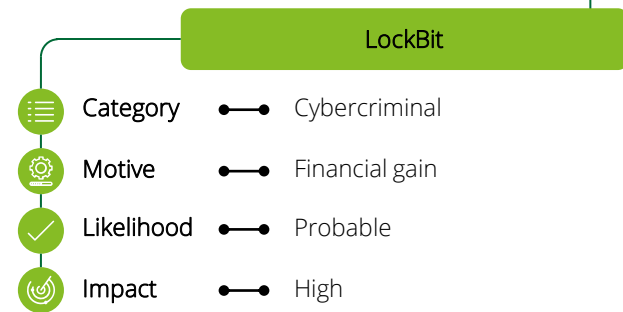
Table of contents

- 1 Executive overview**
High level presentation of top threat actors, threat vectors, incidents, and overall assessment
- 2 Cross-industry threat vectors**
Trending and emerging high-level threat vectors with a global impact
- 3 Trending threat vectors**
Key technical, environmental, and human-centric threat vectors trending globally in 2023
- 4 Initial access techniques**
The most prevalent initial access techniques threat actors use to compromise target systems
- 5 Threat vector highlights**
Spotlight on Artificial Intelligence and malware trends in 2023 as observed by Deloitte
- 6 Threat actors**
High level overview of categories, heatmap, and trending and emerging threat actors with a global impact

Executive overview | Cyber threat trends 2023

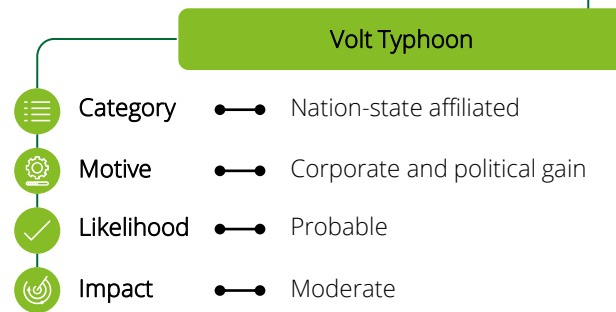
The following report highlights overarching cyber trends and emerging issues from January 1, 2023, to December 31, 2023.

Most impactful threat actor



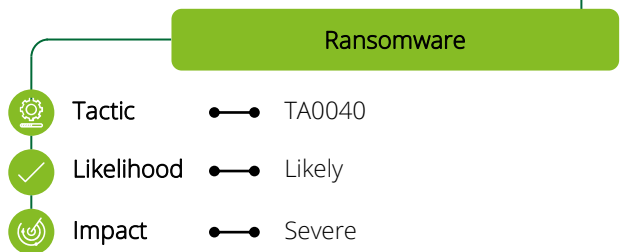
LockBit is agile, evading law enforcement and targeting all industries globally. LockBit operates a very successful Ransomware-as-a-service (RaaS) model. [3]

Most trending threat actor



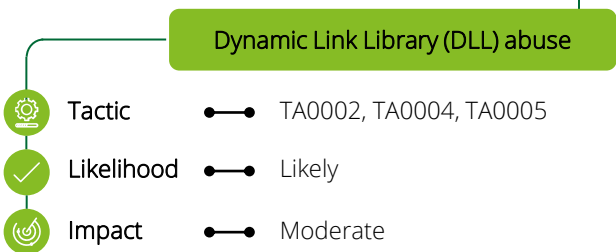
Volt Typhoon lifted the defense evasion bar with their living-off-the-land (LOTL) techniques. They perform stealthy cyber espionage campaigns across multiple industries. [107]

Top threat vector



Ransom demand reached up to \$80 million in 2023, but in an encouraging trend, some businesses – in collaboration with law enforcement – are no longer paying the ransom. [2]

Top trend observed by operations



Operations noted Dynamic Link Library (DLL) abuse through infected Universal Serial Bus (USB) drives, highlighting the persisting trend of threat actors re-using old methods and infrastructure. [1]

Highlights

- Ransomware affected 66 percent of organizations in 2023. [112] Law enforcement agencies globally continue to apply pressure on ransomware groups and Deloitte CTI observed a decrease in the number of ransoms being paid. [7]
- Identity-based initial access techniques are prevalent. Abuse of valid credentials in 2023 accounts for 44.7 percent of all data breaches, up from 41.6 percent in 2022. [15] Protecting valid credentials is paramount for security; this technique facilitates multiple steps in the intrusion chain.
- Threat actors continue to mix new and old techniques. Deloitte teams identified malware spreading through infected USB drives, and threat actors using old source code to create new variants of Mirai and Bashlite to target comparatively new Internet of Things (IoT) infrastructure. [1]

Assessment

- Despite a decline in ransomware payments being made globally, Deloitte CTI assesses with high confidence that ransomware will remain a formidable threat in 2024. As ransomware tactics become increasingly complex and negotiations more aggressive, we expect to see more groups employing the double and triple extortion tactics in a bid to pressure payment.
- Deloitte CTI assess with high confidence that sophisticated threat actors will continue to use zero-day vulnerabilities to target multiple organizations. Software companies that dominate the market are particularly attractive, as threat actors can leverage a single vulnerability affecting multiple organizations, fuelling concerns around the risks of supply chain compromise.



Cross-industry threat vectors | Trends

During 2023, Deloitte CTI observed several overarching, cross-industry threat vectors, not specific to threat actor type. This slide illustrates the global impact of ransomware, data breaches, globally trending malware trends, and our observations from underground forums and marketplaces.



Ransomware

- Impact: High
- Likelihood: Probable

Details

- Ransomware operators continue to use double-extortion tactics across all industries globally, with the US emerging as the most targeted country in 2023. ALPHV, ClOp, LockBit, and Play ransomware were the most prevalent in 2023.
- Ransomware cost more than \$400 million in the first six months of the year, [113] but Deloitte CTI observed an encouraging decline in ransomware payments globally, particularly in the health care and financial services sectors. Sophisticated ransomware operators are increasingly using zero-day exploits as their initial access vector, with 36 percent of victims ransomed in this way. [3] Valid credential compromise was the second most common entry point for ransomware attacks.
- ALPHV's BlackCat ransomware was targeted by the Federal Bureau of Investigation (FBI) and suffered a five-day disruption, which allowed for 500 decryption keys to be retrieved and shared with the affected entities. [3-5]



Major data breaches

- Impact: Moderate
- Likelihood: Roughly even chance

Details

- In 2023, over 8.2 billion records were breached across all industries, with an average cost of \$4.45 million for 2023. [8] The most prevalent initial attack vectors were phishing and stolen, valid credentials.
- Data and Personally Identifiable Information (PII) is most valuable to cybercriminals who profit by selling it, and nation-state threat actors who perform data collection and various espionage activities in support of their respective national security agendas. For example, personal information is also used in sophisticated social engineering campaigns for high-value executives, or for extortion of security-cleared personnel. Instances of class action against providers who fail to keep customers' data safe were on the rise in 2023. [6-8]



Malware trends

- Impact: Significant
- Likelihood: Likely

Details

- Stealth malware is becoming more prevalent. One example is Snake Malware, discovered in 2023 but in operation worldwide for over 20 years. Snake is associated with the Turla Advanced Persistent Threat (APT) group. [13] Dynamic malware capabilities, where malware behavior changes with each attack, renders traditional Indicator of Compromise (IoC) based detection methods less effective.
- Other notable malware trends in 2023 include InfoStealers used for credential theft from web browsers, cryptocurrency wallets, gaming accounts and Virtual Private Network (VPN) and File Transfer Protocol (FTP) services. Additionally, Deloitte CTI observed the prevalence of IoT malware, predominantly in the manufacturing sector globally. [9-13] This topic is detailed in the Threat Vector Highlight section of this report.



Underground trends

- Impact: Moderate
- Likelihood: Roughly even chance

Details

- The key 2023 trends observed by Deloitte CTI in underground forums included the distribution of databases, both for free and for sale, and many offerings of InfoStealers, Remote Access Trojans (RATs), and drainer malware. Largely used by financially motivated threat actors, 'Crypto drainers' use sophisticated phishing websites to trick users into connecting their cryptocurrency wallets with the attackers' infrastructure. [109]
- Access-as-a-Service (AaaS) offerings through Initial Access Brokers (IABs) have been seen in all sectors. Fraud-as-a-Service (FaaS) is also on offer for most sectors.
- In the context of the Middle East conflict, Deloitte CTI also observed threat actors advertising databases and accesses primarily targeting government and corporate networks. [1]

Trending threat vectors | Security operations observations

The following threat vectors encompass a range of technical, environmental, and human-centric approaches that threat actors leverage to conduct malicious cyber activities. These insights were gathered with input from Deloitte’s Security Operations Center (SOC) teams.




Zero-day exploits

Impact Severe

Likelihood Roughly even chance

Details

- In 2023, Deloitte CTI has noted a trend where threat actors are focusing on, and becoming proficient at, exploiting zero-day vulnerabilities in internet-facing edge devices such as firewalls and Virtual Private Network (VPN). Threat actors leverage the fact that security teams often have less monitoring in edge devices. This strategy, consistently used by espionage and ransomware actors, serves to facilitate their operations and maintain undetected access for longer.
- Notably, zero-day exploitation in managed file transfer (MFT) services was prevalent in 2023, mostly impacting US-based organizations. Deloitte CTI has observed certain nation state threat actors are more proficient at exploiting zero-days than others. This may be due to the overlapping nature of state-sponsored cyber operations and legislation for reporting discovered zero-days to a central government authority. [22-23]




Dynamic Link Library abuse

Impact Severe

Likelihood Roughly even chance

Details

- Deloitte SOC observations for 2023 uncovered trends with threat actors abusing rundll32 and DLL file abuse tactics. These techniques are used to achieve payload execution, privilege escalation, and defense evasion. Notably, the SOC team has regularly encountered USB DLL infections throughout 2023 delivering the Gamarue malware/botnet family. Gamarue has been spreading ransomware, trojans, and worms since 2011, as threat actors continue to re-use old infrastructure. Despite Gamarue being historically known to spread through phishing emails, drive-by-downloads, and malicious ads, SOC has primarily seen it delivered via infected removable storage devices. Considered obsolete, and often overlooked as low-priority, USB infections continue to be an effective threat vector as seen with the likes of Gamarue and Raspberry Robin in recent years. [1]



Targeting of cloud services

Impact Severe

Likelihood Very likely

Details

- In 2023, the most targeted cloud environments were Software-as-a-Service (SaaS) at 39 percent, and cloud-based storage services at 36 percent. [24] These attacks often lead to data breaches, impacting 39 percent of businesses that experienced cloud-based targeting. [24] Deloitte CTI observed threat actors increasing their use of valid accounts, used to gain initial access in 43 percent of cloud intrusions. [24] Threat vectors specific to cloud include unmanaged attack surfaces, human error, and misconfigurations. The interdependent and multi-layered structure of cloud-based software systems presents a unique challenge in safeguarding software supply chains within cloud infrastructure. This widened attack surface is accompanied by ungoverned access of non-human credentials (Application Programming Interface (API) keys, tokens, service accounts) to core business environments. [25].



Business Email Compromise

Impact Severe

Likelihood Likely

Details

- Business Email Compromise (BEC) was trending in 2023 with the FBI Internet Crime Complaint Centre (IC3) identifying \$51 billion in losses from 2013 to 2022. [26] BEC attacks surpassed malware delivery in the first six months of 2023, increasing by 55 percent in contrast to the final six months of 2022. Additionally, Vendor Email Compromise (VEC) increased by 137 percent in the financial services industry. [26] Threat actors exploit vendor email accounts and mailbox content to craft more effective lures and impersonations of third-parties in the supply chain. Considering VEC attacks are often sent through legitimate (albeit compromised) email accounts, they are nearly impossible for employees and spam filters to detect. VEC is particularly effective because attackers mimic legitimate vendor communications or hijack existing business conversations to encourage recipients to send fraudulent payments or update banking account information. [26-27]

Initial access techniques | Trends

Deloitte CTI observed that the most leveraged initial access techniques in 2023 were phishing, abuse of valid accounts and external remote services, and exploitation of public facing applications. These techniques were the most impactful across all industry sectors and verticals.



Phishing

- Technique — T1566
- Impact — Severe
- Likelihood — Almost certain

Details

- Phishing remains the top initial access vector, with more than two in five of incidents involving phishing as the pathway to compromise. Despite being one of the oldest social engineering techniques, phishing persists due to its proven effectiveness.
- Generative Artificial Intelligence (GenAI) is now aiding cybercriminals to optimize their campaigns. GenAI has been widely adopted by threat actors who have harnessed this technology to generate or fine-tune credible phishing campaigns. These campaigns now feature improved spelling and grammar, along with the integration of data regarding the target company, its leadership, and publicly available information. [14] This topic is detailed in the Threat Vector Highlight section.



Valid accounts

- Technique — T1078
- Impact — Severe
- Likelihood — Likely

Details

- The second most prevalent initial access vector is through valid accounts with stolen credentials. Cybercriminals continue to focus on identity-based initial access tactics with the abuse of valid credentials accounting for 44.7 percent of all data breaches, up from 41.6 percent in 2022. [15] During 2023 there was also a 147 percent increase in access broker advertisements on the dark web with security researchers estimating there is already over 15 billion leaked login credentials circulating online. [15] Linked to valid accounts is the notable trend of Kerberoasting, up 583 percent in 2023, indicating a nearly six-fold year-on-year spike. [15] [16]



External remote services

- Technique — T1133
- Impact — Significant
- Likelihood — Roughly even chance

Details

- Remote access services are versatile and cost effective. By controlling devices remotely from across the globe, security teams save on response costs, travel times, and can receive remote support from third parties and contractors. These reasons are equally as attractive to threat actors with remote access services broadening the attack surface for organizations. This technique is often accompanied by access to valid accounts and is utilized for initial access and lateral movement. It requires a more active approach compared to easily automated phishing. Sophisticated threat actors such as LockBit use this technique as it leaves less evidence of an intrusion as opposed to automated attacks. This technique is also prevalent in supply chain compromises. [17-18]



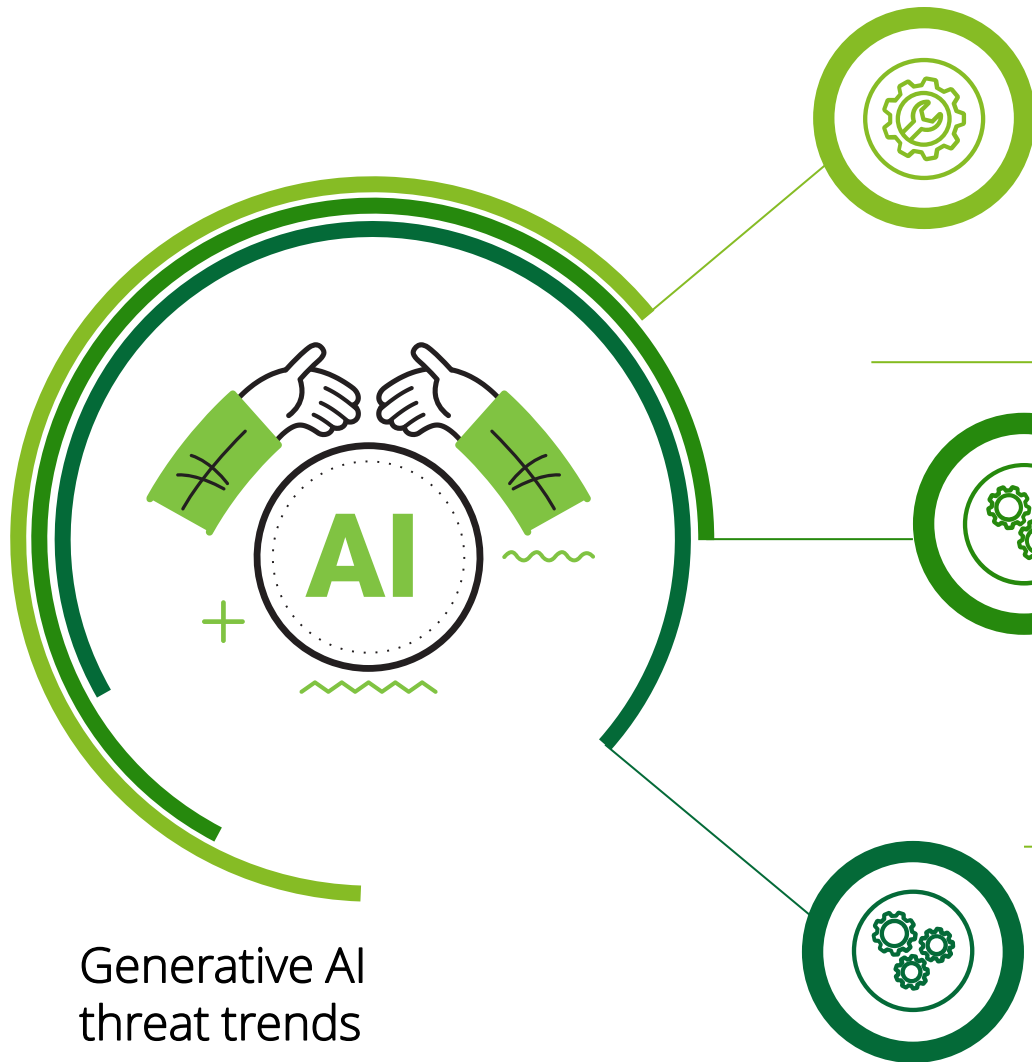
Exploit public facing applications

- Technique — T1190
- Impact — Severe
- Likelihood — Roughly even chance

Details

- Threat actors (e.g., Volt Typhoon, BlackTech, etc.) continue to exploit websites, web servers, structured query language (SQL) services or any other internet facing application. These systems are often targeted due to their availability and accessibility from anywhere in the world. Deloitte's incident response teams have found that most vulnerabilities are due to misconfigured or default settings in these applications, and less so inherent in design flaws, bugs or glitches. This access vector is also susceptible to unpatched vulnerabilities, with Common Vulnerabilities and Exposures (CVEs) from 2021 in exchange servers and VPN services still being exploited in 2023.

Threat vector highlight | Use of AI



Influence Operations (IO)

AI-image deception and deepfakes

- AI-generated images are more visually striking and effective compared to previous campaigns. AI is designed to create compelling and provocative images and improve them over time. [114]. There are two perspectives to this:
 - AI-enabled IO leveraging social media, and
 - AI-enabled IO incorporated in cyberattacks.
- **Use case 1:** State-sponsored threat actors use AI-generated images to spread propaganda on social media.
- **Use case 2:** Threat actors use live deepfake video to pose as an executive and trick a finance employee into sending millions to a malicious account.
- **Use case 3:** Compelling AI-generated images increase employee engagement in phishing campaigns.

Social engineering

Phishing

- AI tools offer threat actors sophisticated capabilities, including generating scam emails. [115]
- AI improves phishing campaigns with more correct grammar, punctuation, and talking points in whaling and BEC campaigns.
- **Use case:** Threat actor uses AI to generate an email that uses language to impersonate an executive in fraud scam.

Vishing: Voice Cloning-as-a-Service (VCaaS)

- Threat actors can use AI-based voice cloning tools in vishing for financial fraud and unauthorized access to systems protected with biometric authentication. [116]
- Threat actors used voice cloning in several schemes, including impersonating a victim's family, impersonating an executive authorizing a financial transaction, or tricking biometric authentication to access a protected system.
- Threat actors can use paid VCaaS tools to conduct vishing operations.
- **Use case:** A threat actor uses a VCaaS tool to clone the voice of an executive or person with authority to approve a financial transaction.

Underground services/ collaboration

AI-as-a-Service

- Deloitte CTI continues to observe threat actors collaborating on underground forums on ways to use AI in scams.
- Malicious AI tools are identifying vulnerabilities for potential exploitation.
- Underground handles have announced personalized AI chatbots designed to create malicious programs.

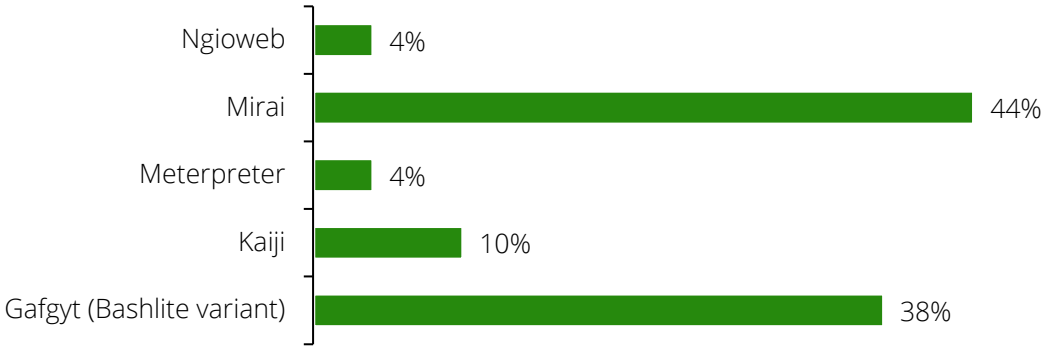
Threat vector highlight | IoT malware trends

Threat of IoT malware in 2023

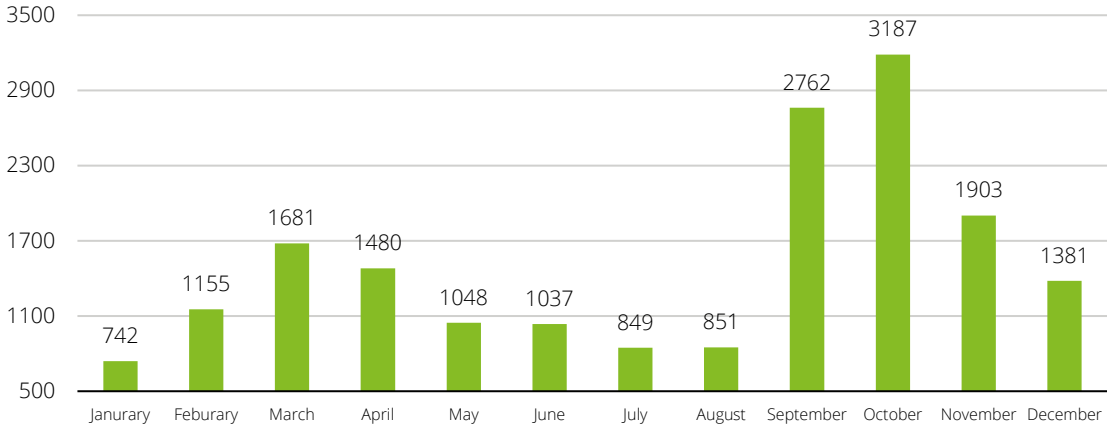
Deloitte CTI has identified a significant surge in malware targeting IoT in 2023, peaking in mid-October. Over the year, 82 percent of IoT malware observed by Deloitte collection belonged to the Mirai and Gafgyt (Bashlite variant) malware botnets (see Figure 1). Independent reporting states that routers were the most targeted (a total of 66 percent), followed by cameras and firewalls (at 7.7 and 5.1 percent respectively). These statistics reveal an overall 400 percent year-on-year (January- June 2023) increase in IoT malware attacks across various industries with the manufacturing industry being the most targeted sector globally. [1] [29]

Cybercriminals are predominantly targeting legacy vulnerabilities, for example improper input validation or Operating System (OS) command injection, with 34 of the 39 most popular IoT exploits aimed at vulnerabilities that have existed for over three years. Proliferation of IoT malware is expected to continue into 2024 as the adoption of interconnected devices grows. Coupled with the proliferation of 5G, the IoT attack surface will continue to garner attention for cybercriminals as an entry point into corporate networks. [28]

Top five IoT malware observed in 2023



IoT malware observed in 2023



Mirai Botnet Highlight

The Mirai botnet is infamous amongst IoT malware families. Identified in 2016, it has made a comeback in 2023, with multiple variants used in various attacks:

- NoaBot variant used in crypto mining since the start of 2023 [32]
- Medusa malware-as-a-service (MaaS) variant with a ransomware module in February [34]
- IZ1H9 variant targeting Linux routers in September [33]

The Mirai botnet continues to live on through its public source code, with cyber criminals creating mutated variants. With the current number of connected IoT devices already surpassing 16.7 billion and an anticipated surge to 29 billion by 2027, the threat posed by IoT malware looms large for any organisation as we navigate Industry 4.0. [30] From late September to October, Deloitte CTI observed a surge in the Mirai botnet attacks (see Figure 2). Spiking in September, Deloitte CTI monitored the appearance of three rapidly spreading botnet variants originating from the Mirai variant dubbed by researchers as - HailBot, KiraiBot, and CatDDoS. Further strengthening the surge of attacks, the InfectedSlurs botnet campaign began exploiting two zero-day vulnerabilities in network video recorders around the same time. [29-31]

Threat actors | Overview



Nation-state linked

- Motivation** — Political, Espionage, Financial
- Likelihood** — Likely, Significant long-term impact
- Top Actors** — BlackTech, Volt Typhoon, Maui ransomware, Lazarus Group

- Nation-state sponsored APT groups pose the most significant long-term cybersecurity threat, as their presence on a compromised system may go unnoticed for months or years. This can undermine the credibility of an entire sector or industry.
- In 2023, the line between politically and financially motivated threat actors' interests blurred. There is a trend of nation-state sponsored threat actors collaborating with cybercriminals in a multi-pronged approach to achieve their desired outcomes. For example, as the definition of critical infrastructure expands to include financial services, the motivation of nation-state sponsored threat actors and cybercriminals will become fuzzier. [47][62-66] [79] [107]



Cybercriminals

- Motivation** — Financial
- Likelihood** — Likely, Significant immediate impact
- Top Actors** — LockBit, ALPHV/Blackcat, Play Ransomware, Akira Ransomware

- Cybercriminal activity can produce an immediate impact, affecting production services and reputation. RaaS and the prevalence of a few highly active and disruptive ransomware families persisted in 2023. In line with RaaS, Initial Access Brokers (IABs) services have also experienced significant demand.
- Cybercriminal communications using chat applications over dark web forums also persisted. This pivoting is possibly due to sustained law enforcement action against dark web forums and marketplaces
- Finally, multi-purpose malware, including IoT malware proliferated by cybercriminals remains prevalent worldwide. [67-68]



Hacktivists

- Motivation** — Political
- Likelihood** — Roughly even chance, Moderate impact
- Top Actors** — SiegedSec, Five Families (Blackforums, GhostSec, SiegedSec, Stormous, and ThreatSec)

- Politically motivated hacktivists once again demonstrated their ability to mobilize, this time in the context of the Middle East conflict. This threat manifests in the form of website defacement and distributed denial-of-service (DDoS) attacks of their targets' web portals, with the occasional leak of stolen information. The scale of civilians involving themselves in military conflict through cyber means resulted in the International Committee of the Red Cross (ICRC) issuing its first ever ethical guidelines for "civilian hackers."
- Other hacktivist groups such as SiegedSec and Five Families are showing a trend similar to RaaS providers by forming more organized alliances to enhance reach and capability. [69-70]

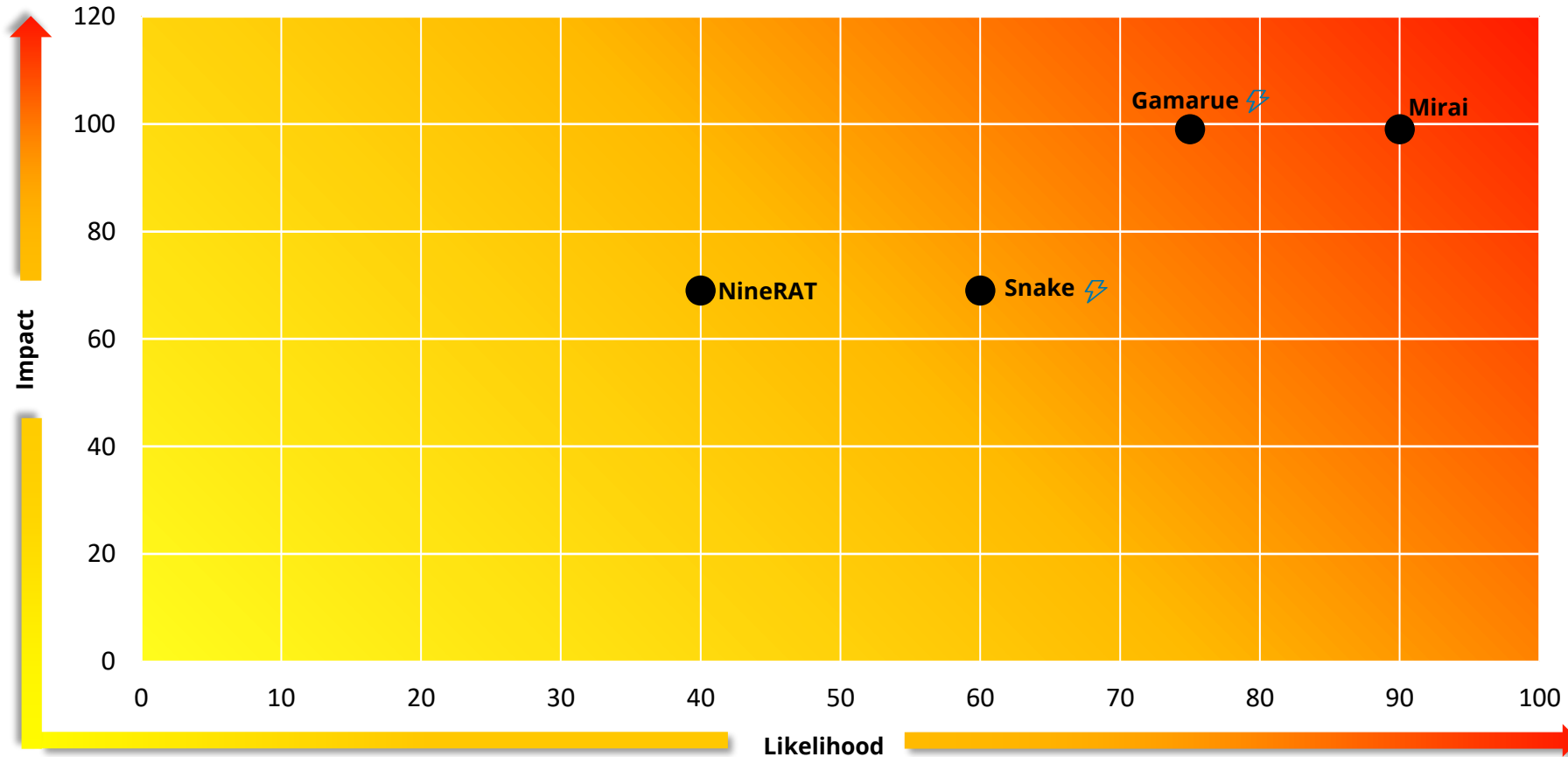


Insider threat

- Motivation** — Financial, Revenge, Fear (blackmailed)
- Likelihood** — **Malicious:** Roughly even chance, Severe impact
Unintentional: Likely, Significant impact
- Top Actors** — "bronzegods"; "I_Deleter"; "neboltay"; "Jolbit08"; "lies"; "Enony";

- Throughout 2023, Deloitte CTI observed threat actors actively recruiting insiders on dark web forums.
- Global economic pressures provide motivation for affected individuals to engage in malicious activity for financial gain, and threat actors leverage economic uncertainty in their insider recruitment efforts.
- Threat actors also sought to recruit insiders from within government organizations, financial institutions, mobile carriers (to facilitate subscriber identity module (SIM)-swapping), and other major companies worldwide, for intelligence collection and espionage purposes. [71]

Malware | Trending and emerging in 2023

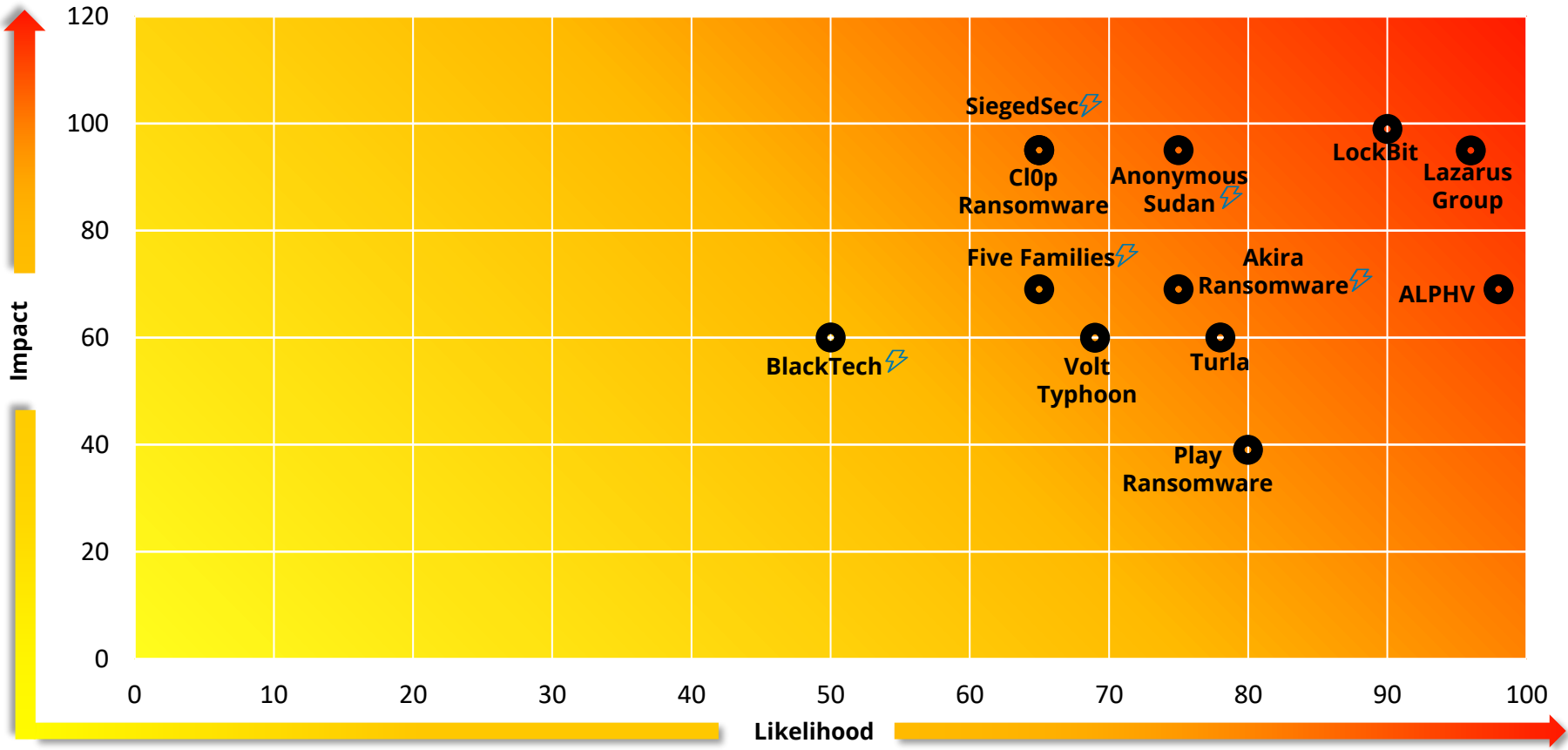


This image highlights the most active and impactful malware families over the last year in both frequency and spread of campaign, as well as newly emerging, as applicable to this report. Deloitte CTI analysts conducted a probability-based risk assessment to provide contextual risk quantification for the threat actors that meet these criteria. The team used specific, scenario-based questionnaires to assess the threat for each actor. The value for each scenario was customized based on its criticality.

“Emerging” means the malware has begun activity in the past 12 months. “Re-emerging” means that the malware have been inactive for more than six months prior to the reporting period and has recently become active again.

 Re/Emerging Malware

Malware | Trending and emerging in 2023



This image highlights the most trending and impactful threat actors over the last year in both frequency and spread of campaign, as well as newly emerging. Deloitte CTI analysts conducted a probability-based risk assessment to provide contextual risk quantification for the threat actors that meet these criteria. The team used specific, scenario-based questionnaires to assess the threat for each actor. The value for each scenario was customized based on its criticality.

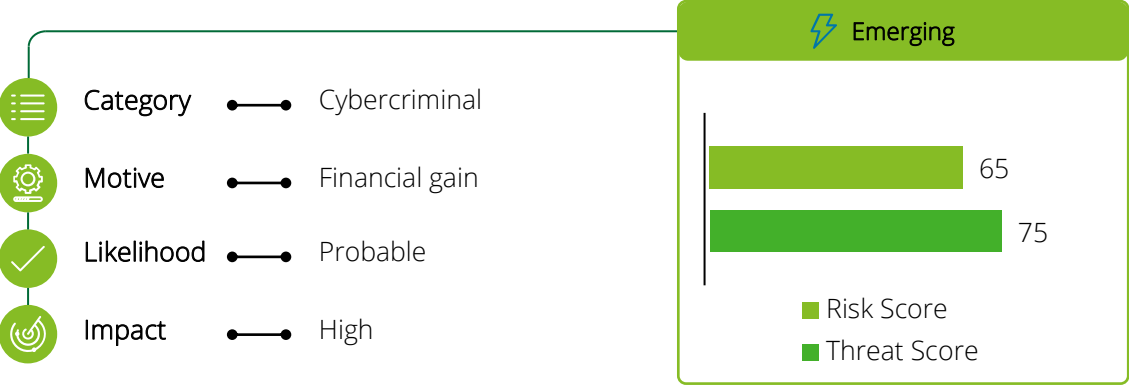
“Emerging” means the threat actor has begun activity in the past 12 months. “Re-emerging” means that the threat actors have been inactive for more than six months prior to the reporting period and have recently become active again.

Re/Emerging Malware

Threat actor profiles | Trending and emerging



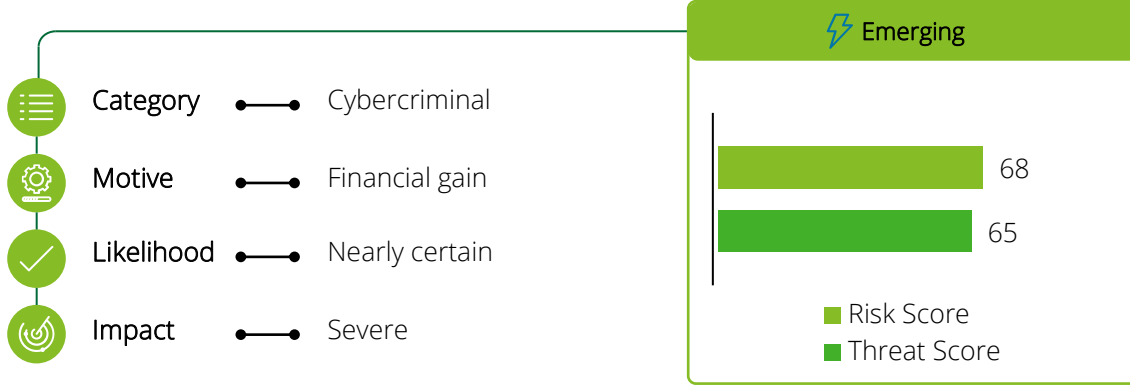
Akira Ransomware



- Akira is a ransomware threat actor group that was first observed late March 2023. Akira operate as a RaaS scheme for personal gain and use double extortion.
- Targeted sectors include transportation businesses of small to medium size where ransoms demanded range between \$200,000 to \$4 million.
- Akira predominantly uses compromised credentials, possibly obtained from their affiliates or from phishing or spear-phishing campaigns. Akira also exploits poorly configured Remote Desktop Protocol (RDP) connections to gain access to accounts, including those with Multi-Factor Authentication (MFA) enabled. To establish persistence, they install remote management software.
- In the first half of 2023, Akira targeted 60 organizations worldwide and listed victims and their stolen data on their Tor site. More recently, in August, Akira added a US/Canadian transportation services company which offers switching and terminal services to its data leak site. Over 85GB worth of sensitive information was exfiltrated. [72-75]



ALPHV

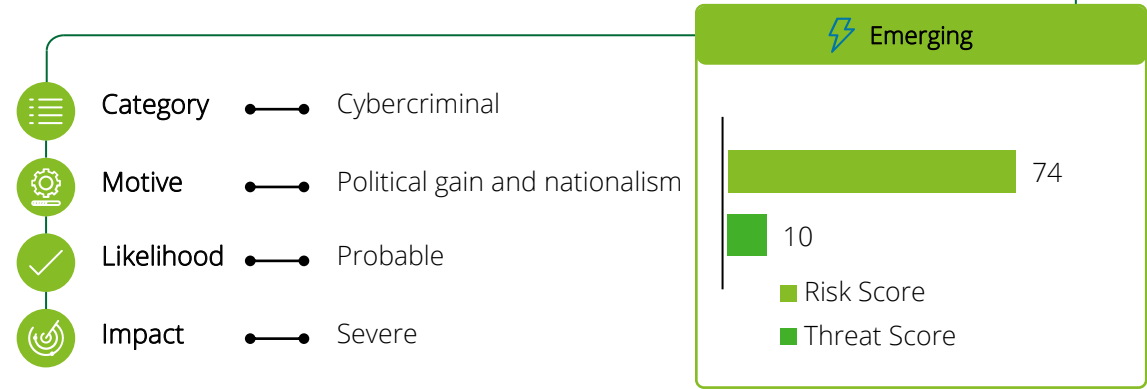


- ALPHV is a cybercriminal threat actor first observed in 2021. The group operates under a RaaS model and are financially motivated. They engage in big game hunting (BGH) operations across multiple countries.
- Targeted sectors include financial services, logistics, commercial, construction, energy, manufacturing, pharmaceutical, retail and technology.
- ALPHV uses its rust-based namesake ransomware (BlackCat) to conduct operations across various OSS and cloud environments. In February 2023, they released and promoted the BlackCat Ransomware 2.0 Sphinx update, designed to provide better d evasion and additional tooling.
- The group is proficient in lateral movement and are thorough in operational security (OPSEC) by deleting shadow copies with VSSadmin and emptying recycle bin. To exfiltrate information, ALPHV use MEGAsync, Exmatter and Rclone which mimic processes and are disguised by their names.
- In December 2023, the FBI seized the group's servers and obtained their private decryption keys, assisting over 400 victims to recover their stolen files. As of January 2024, Deloitte CTI observed ALPHV reclaimed their site and remain active. Then in February 2024, ALPHV claimed it was shut down by law enforcement, but this under dispute and the status of the group is uncertain. [60-61] [76-78]

Threat actor profiles | Trending and emerging



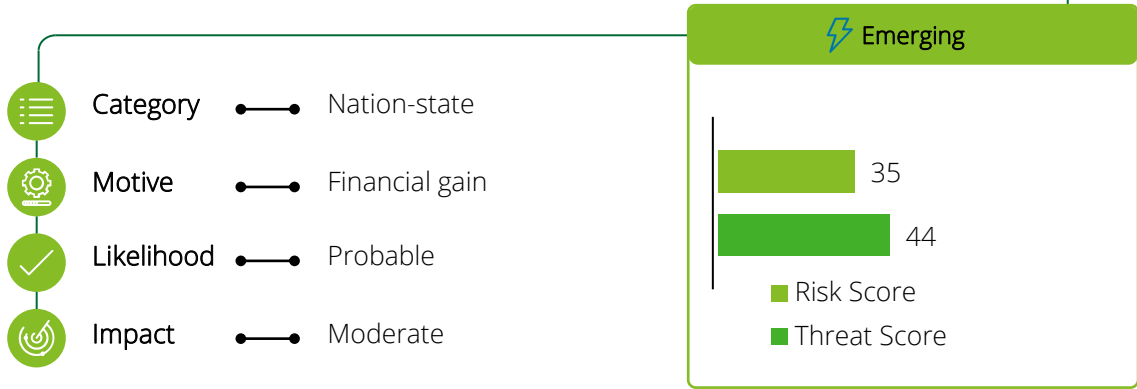
Anonymous Sudan



- Anonymous Sudan, first observed in January 2023, claims to be a Sudanese hacktivist group motivated by religious and political beliefs. Despite the group's claims, security researchers believe Anonymous Sudan is a pro-Russian hacktivist group, with the majority of their attacks focusing on Australia, Europe, Israel, and the US. In contrast to the religious persona behind the attacks, security researchers have observed Anonymous Sudan teaming up with Russian threat actors Killnet and REvil to carry out attacks alluding to the possibility of Anonymous Sudan being a masked subsidiary of Killnet, driven by pro-Russian beliefs. [110-111]
- Anonymous Sudan performs Hypertext Transfer Protocol (HTTP) flood DDoS attacks, designed to overwhelm a targeted server with requests, taking target infrastructure offline. The group uses paid infrastructure rather than leveraging botnets to carry out these attacks. By leveraging a cluster of rented servers, the output produces more traffic than personal devices. This highlights the group's wealth of financial resources, leading security experts to believe the group are not the grassroots hacktivists they claim to be.
- Anonymous Sudan has also been known to make threats via public announcements and propaganda, though attacks have not been carried out as expected in all claimed cases. The group likely uses this method to gain attention for their ideological motives and to sow uncertainty amongst potential targets. [1] [110-111]

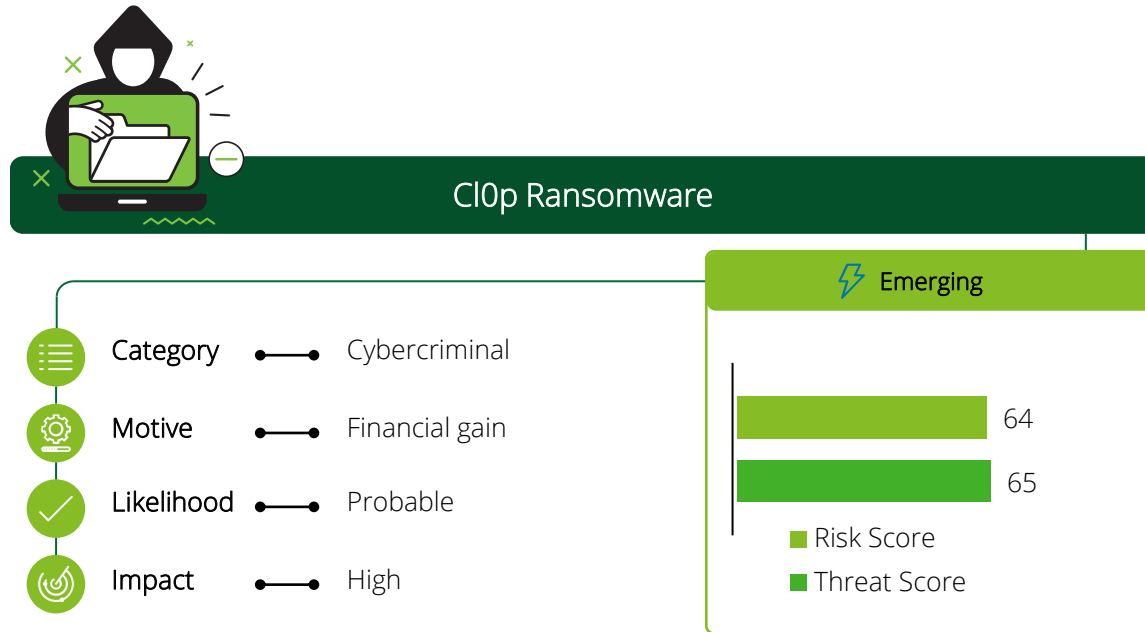


BlackTech

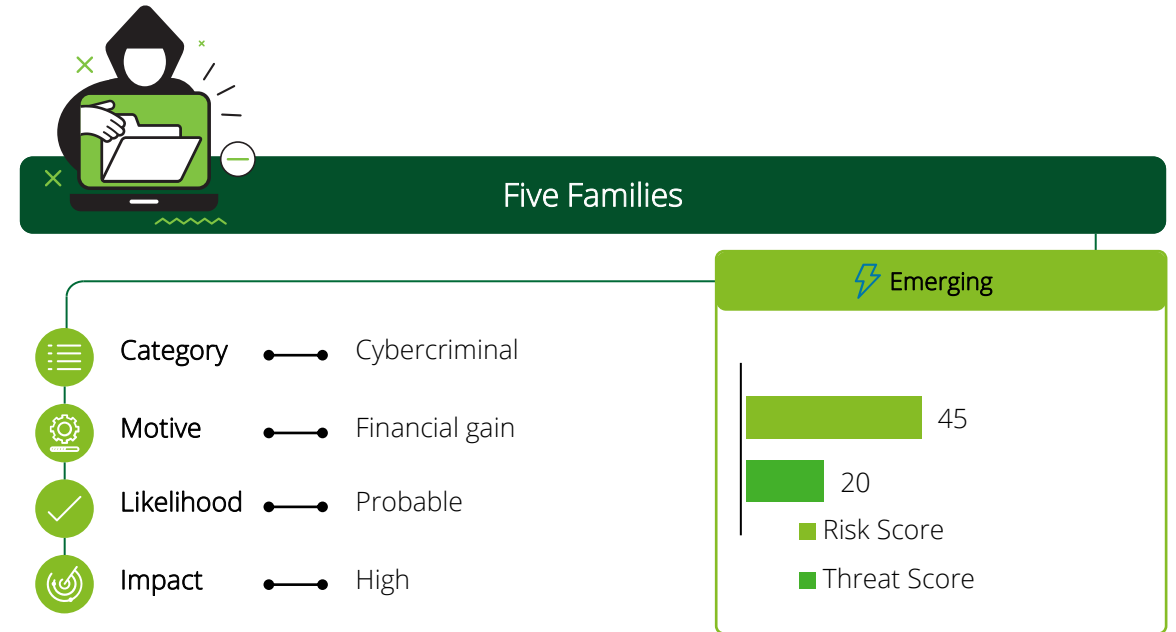


- BlackTech is a suspected Asian nation-state linked cyber espionage group that has been operating since at least 2010, conducting campaigns against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong, as well as some targets in the US.
- The group has shown a particular interest in targeting finance, media, construction, technology, electronics, telecommunications, and health care industries within the private sector, and targeting organizations working with the US and Japanese militaries for the purpose of cyber espionage and to gain sensitive information.
- Across its campaigns, the group has used a mix of both custom and legitimate tools and LOTL techniques, including disabling logging on routers to assist in concealing their operations. Some of the group's custom malware used in exploiting routers include SpiderPig, BendyBear, Bifrose, FrontShell and FlagPro.
- In September 2023, the group was observed modifying router firmware to conceal its activity of targeting companies based in the US and Japan. BlackTech actors typically exploit trusted network relationships between an established victim and other entities to explain their access in target networks. After gaining initial access into a target network, the group escalate privileges in network edge devices and modify the firmware to hide their activity and maintain persistence in the network. [79-81]

Threat actor profiles | Trending and emerging



- The CI0p ransomware group has been active since at least February 2019 and is suspected to be operated by the financially motivated, TA505 and FIN11 threat actors. The group operates under the RaaS model and recruit affiliates.
- CI0p mainly targets the industrial, financial and technology sectors.
- CI0p's victims are mainly located in the US, although it has also been known to target other countries including Australia, Brazil, Canada, Hong Kong, New Zealand, and the United Kingdom.
- Since 2020, CI0p functions under a double extortion scheme which can be upgraded to a quadruple extortion scheme. The group manages its own data leak site, which can be accessed via Tor and typically issue high ransom demands that can escalate up to tens of millions of dollars.
- In late January, CI0p exploited a zero-day RCE vulnerability (CVE-2023-0669) in the MFT service. A working exploit was released on February 6, leading to a 91 percent increase in ransomware attacks by May, mostly affecting the US.
- In May, CI0p exploited a zero-day SQL injection vulnerability (CVE-2023-34362) in the MFT service. This impacted over 2000 organizations and approximately 60 million individuals' data, predominantly in North America (approximately 88 percent) and Europe. [39-41] [48-50]

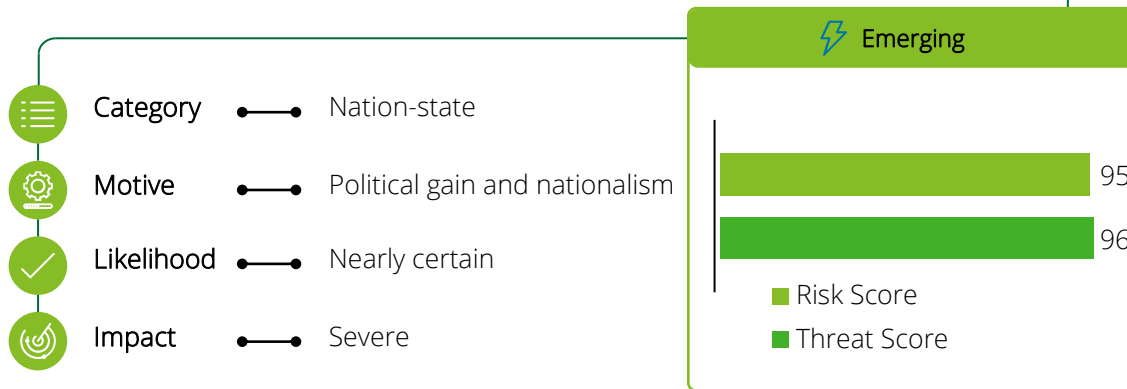


- Five Families is a threat actor alliance founded in August 2023 by the standalone hacktivist groups Blackforums, GhostSec, SiegedSec, Stormous, and ThreatSec. They target both public and private-sector organizations globally.
- Some of the members, such as GhostSec, adopted a vigilante stance with regards to the on-going Middle East conflict. [84]
- The threat actor alliance frequently launch ransomware attacks and extort the victims for their data. They have openly acknowledged involvement in a cyber attack against a global computer hardware accessories manufacturer headquartered in Asia.
- In August 2023, they launched a cyber attack on a South American automation company, claiming to access 230GB of data from the company's cloud systems. This data allegedly contained customer data, financial information, internal documents and company software. In December, Five Families as a collective released a data leak from an Asian clothing store that involved over one million records with internal system logs and personal employee documentation.
- The Five Families collective is a prime example of the increasing trend in threat actor collaboration, in favor of enhanced capabilities and knowledge sharing, resulting in more impactful attacks. [82-85] [87]

Threat actor profiles | Trending and emerging



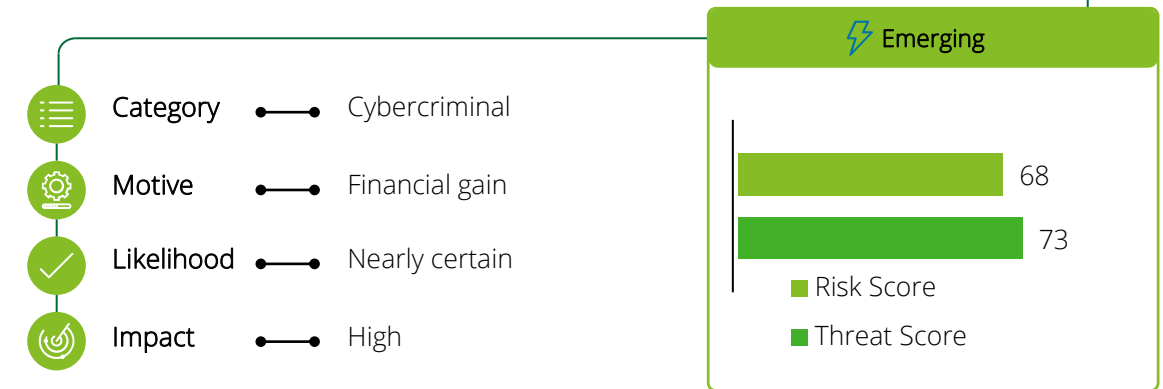
Lazarus Group



- Lazarus Group is a suspected East Asian nation-state threat actor, first observed in 2009. They are primarily tasked with obtaining strategic information that facilitates espionage activity. The group works closely with other threat actors such as Bluenoroff and Andariel; likely subgroups of Lazarus.
- Targeted sectors include banking institutions, cryptocurrency exchanges and other financial services, and casinos.
- The group uses multiple operations to achieve their aim, including distributing fake job offers via email in phishing schemes. They have also impersonated legitimate job recruiters through setting up illegitimate accounts.
- Lazarus Group have used custom malware to target various operating systems and typically feature persistence mechanisms and apply anti-detection techniques.
- Lazarus Group has stolen an addition \$100 million this year in cryptocurrency. In December, they released new RAT malware by utilizing a Log4j bug that is over two years old.
- The group continues to exploit CVE-2021-4428, through the deployment of NineRAT and DLRAT in December 2023, along with a malware downloader named BottomLoader [88-90]

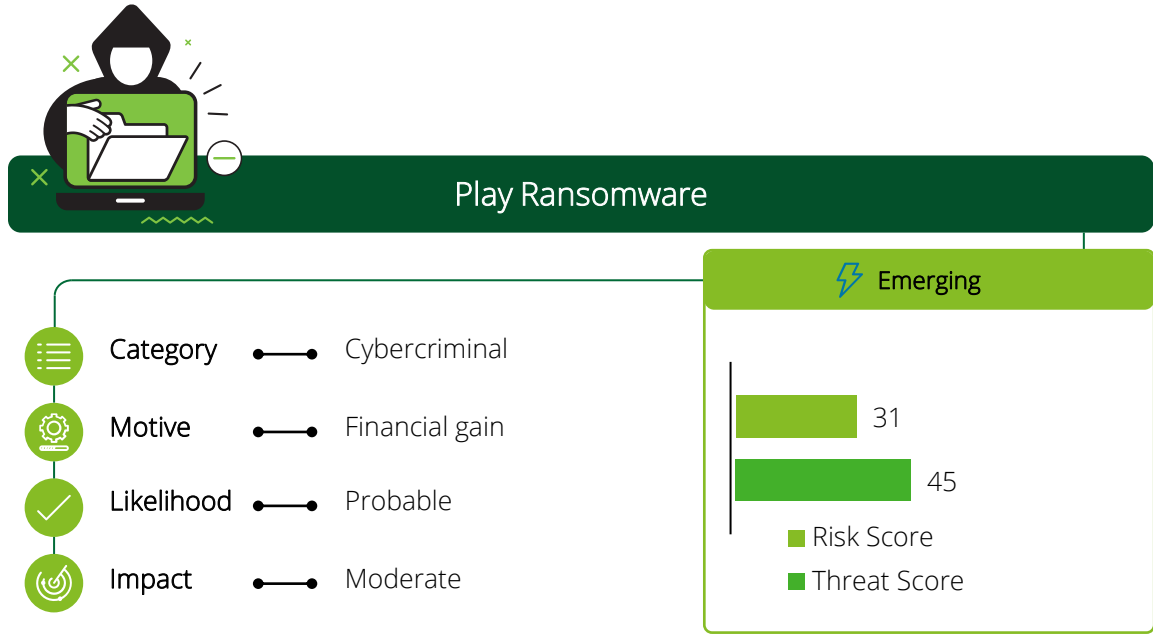


LockBit

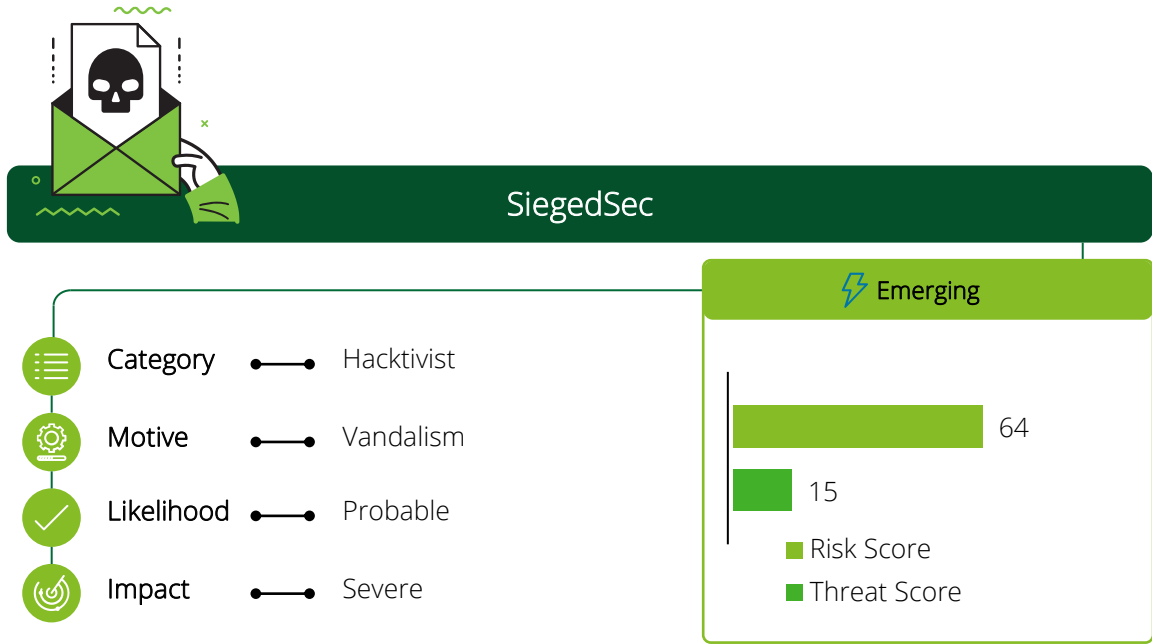


- LockBit is a ransomware threat group first observed in 2019 that is suspected to have originated from Eastern Europe. The group operates in a RaaS model, under which they recruit affiliates in return for a fraction of the ransom obtained from each attack. US and global law enforcement agencies took over LockBit's website, servers, and disrupted its operations in February 2024 but LockBit's leaders rebuilt its infrastructure and resumed ransomware operations days later.
- The group targets a variety of industry sectors including financial services, communications, commercial and retail globally. Notably, LockBit variants made up nearly 28 percent of all known ransomware attacks from July 2022 to June 2023.
- LockBit tactic highlights: T1486 - Data Encrypted for Impact, and T1005 - Data from Local System. These tactics require high technical ability to search local system sources to find files of interest and sensitive data prior to exfiltration, as well as LockBit's skill to encrypt data on target systems – interrupting availability to that system and network resources. It is also worth noting that these tactics are more likely to be seen in ransomware attacks. [91-94]

Threat actor profiles | Trending and emerging

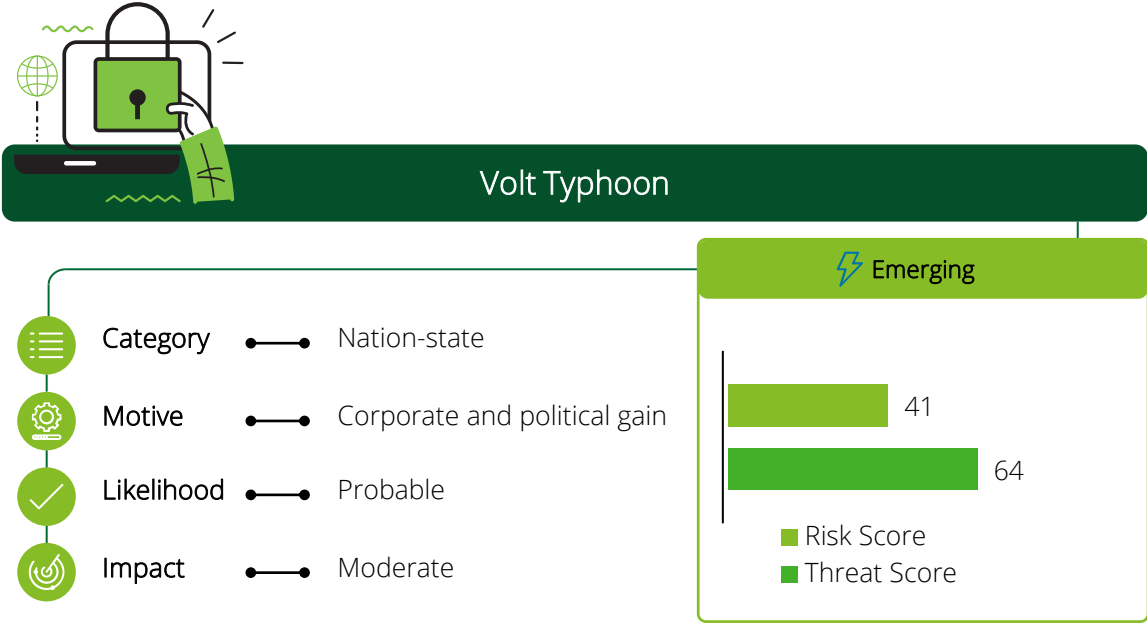
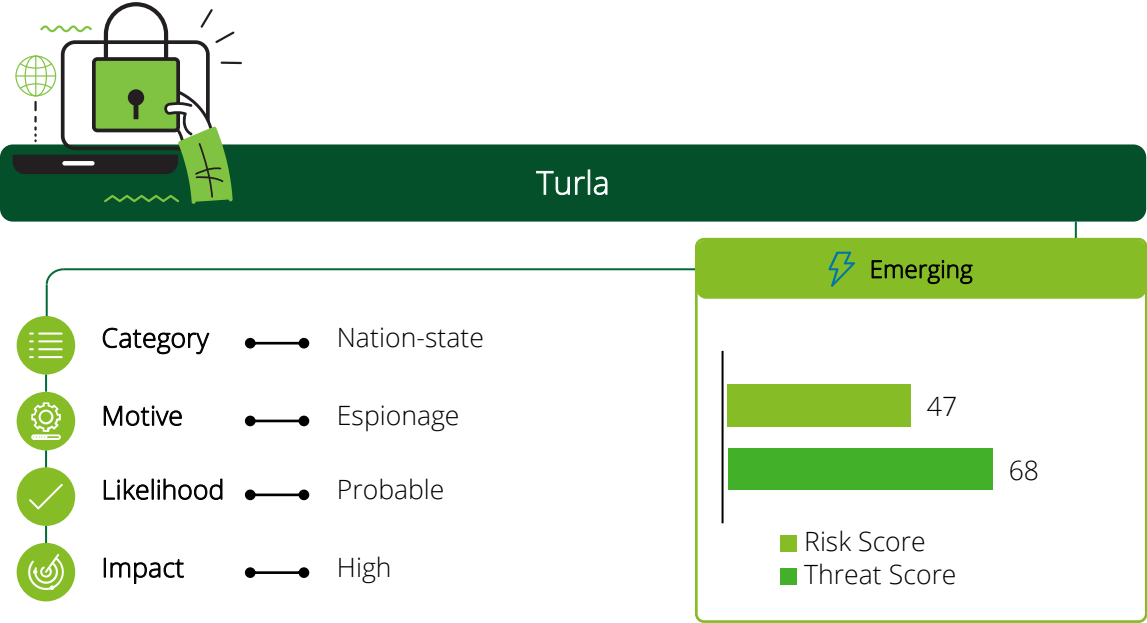


- Play Ransomware is a suspected Eastern European cybercriminal actor group, first observed in 2022. They are financially motivated and have launched attacks against public-facing RDP servers and exploit vulnerabilities in Secure Sockets Layer (SSL) VPNs.
- Targeted sectors include energy, government, insurance, manufacturing, media, retail and technology.
- Play's encryption methods are similar to other Eastern European ransomware groups such as Hive and Nokoyama.
- In January 2023, Play used compromised accounts to remotely authenticate into a British-based security software and hardware company and began reconnaissance activities. They retrieved two .ZIP files and binaries. After 14 days, they tampered with the system's Group Policy Object (GPO) settings which resulted in leveraging the cmd.exe to launch Play ransomware across infected devices.
- Between August and November, a range of counties were compromised with consistent tactics used to attack organizations, infecting systems with malicious files in the 'Music' directory. This involved over 300 victims' information put on a data leak site. [95-98]



- SiegedSec is a hactivist group that has been active since 2022. The group mainly targets government entities and disrupts critical infrastructure organizations, including healthcare and commercial organizations.
- SiegedSec is suspected to collaborate with another threat actor, GhostSec, specifically in operations targeting Colombia, Israel and the US.
- The threat actor's attacks include defacement and website compromise, leaking sensitive information and gaining unauthorized access to databases and emails. These attacks often include crude language and graphics using SQL injection and Cross-Site Scripting (XSS).
- In early 2023 they compromised an Australian software company and released personal information relating to over 10,000 employees.
- In May 2023, the hactivist group claimed responsibility for a series of attacks against government entities in South America. In June, SeigedSec announced that it had compromised a South American country's Ombudsman office, and exfiltrated approximately 6GB worth of internal documents, emails and information from the agency's case investigation search engine. In December, they also allegedly stole from unnamed US government entities which resulted in compromised information belonging to US citizens including full names, phone numbers, email addresses, and home addresses. [99-105]

Threat actor profiles | Trending and emerging



- Turla is an APT group suspected to be related to the Federal Security Service of the Russian Federation (FSB) and has been active since as early as 2005. [106] Their suspected motive is intelligence gathering, based on their chosen targets, the use of at least one zero-day exploit, a large network of compromised websites, and the advanced nature of the malware used.
- The group utilizes sophisticated malware to target government-related entities in many countries systematically. Along with this, the group uses highly-targeted spear-phishing and watering-hole attack campaigns to target its victims. The group as also been noted for its zero-day exploits and signing its malware with stolen certificates.
- Once the group gains a foothold into a victim's environment, the focus is shifted to long-term persistent monitoring tools which exfiltrate data and can also provide powerful spying capabilities. The group's primary targets include government institutions, embassies, education and research facilities.
- On May 9, 2023, the US Department of Justice announced the disruption of the global peer-to-peer (P2P) network of devices infected with the Snake malware, attributed to the group. The operation, successfully neutralized the malware using a tool developed by the FBI, which established communication sessions with Snake samples and issued commands to disable them without affecting the compromised systems. Authorities communicated that the Russian government used Snake for twenty years to conduct cyber espionage on North Atlantic Treaty Organization (NATO) members and journalists, leaking confidential documents through a global network of infected devices. [1][45-46][106]

- Volt Typhoon is a suspected East Asian nation-state threat actor first observed in mid-2021. The group perform cyber espionage campaigns mainly targeting Guam Island and the US.
- Targeted sectors include communications, construction, government, education, maritime, manufacturing, utilities, technology and transportation.
- Volt Typhoon demonstrated stealthy capabilities, heavily utilizing LOTL techniques and hands-on-keyboard activity. Some of the observed techniques include routing malicious traffic through compromised office network equipment and deploying modified variants of open-source tools to establish Command and Control (C2) communication. The group's attacks involve credential theft to maintain persistence and the network discovery in critical infrastructure organizations.
- In May 2023, the group ran a campaign aimed at disrupting critical communications between the US and Asia. To gain initial access the group leveraged privileges from extracted credentials to an Active Directory (AD) account used by the device and then attempted to authenticate to other devices on the network with these credentials. [107-108]

Sourcing Statement

Tradecraft: We apply the Intelligence Community Directive (ICD) 203 Analytic Standards to our products and reports, as well as other intelligence community-based tradecraft such as combating biases, techniques for analysis (i.e., alternatives, competing hypothesis), and sourcing disclosures.

Methodology: Our risk ratings are based on weighted factors, including threat actor sophistication, campaigns, frequency of employment, regional spread, and motivation.

Collection: We combine our proprietary collection with subscriptions to ensure maximum coverage and collection for helping prevent threats, including a malware repository, threat library, and underground and dark web accesses.

		Impact				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood	Almost no chance (1-5%)	Low	Low	Low	Low-Medium	Medium
	Very Unlikely (5-20%)	Low	Low	Low-Medium	Medium	Medium
	Unlikely (20-45%)	Low	Low-Medium	Low-Medium	Medium	Medium-High
	Roughly even chance (45-55%)	Low	Low-Medium	Medium	Medium-High	Medium-High
	Likely (55-80%)	Low	Low-Medium	Medium	Medium-High	High
	Very likely (80-95%)	Low-Medium	Medium	Medium-High	High	High
	Almost certain (95-99%)	Medium	Medium-High	High	High	High

Sources

1. Deloitte internal sources.
2. Odiesa, M., "Top 8 largest ransomware demands of 2023," Network Tigers, January 4, 2024. [Online]. Available: <https://news.networktigers.com/all-articles/top-8-largest-ransomware-demands-of-2023/>. [Accessed: January 22, 2024].
3. Staff, "A Comprehensive List of Top Ransomware Attacks in 2023," Sangfor, January 02, 2024. [Online]. Available: <https://www.sangfor.com/blog/cybersecurity/list-of-top-ransomware-attacks-in-2023> [Accessed: January 16, 2024].
4. Staff, "2023 Ransomware Attacks Up More Than 95% Over 2022, According to Corvus Insurance Q3 Report," DarkReading, October 25, 2023. [Online]. Available: <https://www.darkreading.com/cyberattacks-data-breaches/2023-ransomware-attacks-up-more-than-95-over-2022-according-to-corvus-insurance-q3-report> [Accessed: January 16, 2024].
5. Abrams, L, "The Week in Ransomware - December 22nd 2023 - BlackCat hacked," BleepingComputer, December 22, 2023. [Online]. Available: <https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-22nd-2023-blackcat-hacked/> [Accessed: January 16, 2024].
6. Staff, "Latitude Financial Data Breach Investigation," Hayden Stephens and Associates, no date. [Online]. Available: <https://www.latitudedatabreach.com.au/> [Accessed: January 23, 2024].
7. Staff, "Cost of a Data Breach Report 2023," IBM, no date. [Online]. Available: <https://www.ibm.com/reports/data-breach> [Accessed: January 25, 2024].
8. Ford, N, "List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached" IT Governance, January 5, 2024. [Online]. Available: <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023> [Accessed: January 25, 2024].
9. Freed, A., "Indicators of Behaviour and the Diminishing Value of IOCs," Cybereason, no date. [Online]. Available: <https://www.cybereason.com/blog/indicators-of-behavior-and-the-diminishing-value-of-iocs>. [Accessed: January 23, 2024].
10. Staff, "The growing threat from infostealers," Counter Threat Unit Research Team, Secureworks, 2023. [Online]. Available: <https://www.secureworks.com/research/the-growing-threat-from-infostealers>. [Accessed: January 23, 2024].
11. Staff, "A Detailed Analysis of the RedLine Stealer," Security Scorecard, no date. [Online]. Available: <https://securityscorecard.com/research/detailed-analysis-redline-stealer/> [Accessed: January 23, 2024].
12. Staff, "Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service," Office of Public Affairs, US Department of Justice, May 9, 2023. [Online]. Available: <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled>. [Accessed: January 23, 2024].
13. Staff, "Hunting Russian Intelligence Snake Malware," Joint Cybersecurity Advisory AA23-129A, May 9, 2023. [Online]. Available: https://media.defense.gov/2023/May/09/2003218554/-1/-1/0/JOINT_CSA_HUNTING_RU_INTEL_SNAKE_MALWARE_20230509.PDF. [Accessed: January 23, 2024].
14. Gold, J, "Email phishing still the main way in for hackers: report," CSO, August 15, 2023. [Online]. Available: <https://www.csoonline.com/article/649551/email-phishing-still-the-main-way-in-for-hackers-report.html> [Accessed: January 9, 2024].
15. Staff, "2023 Data Breach Investigations Report," Verizon, June 06, 2023. [Online]. Available: <https://www.verizon.com/business/resources/Tcd5/reports/2023-data-breach-investigations-report-dbir.pdf> [Accessed: January 21, 2024].
16. Staff, "Amid Sharp Increase in Identity-Based Attacks, CrowdStrike Unveils New Threat Hunting Capability," CrowdStrike, August 24, 2023. [Online]. Available: <https://www.crowdstrike.com/blog/crowdstrikes-fight-against-identity-based-attacks> [Accessed: January 10, 2024].
17. Greig, J., "Human-operated ransomware attacks tripled over past year," The Record, October 06, 2023. [Online]. Available: <https://therecord.media/human-operated-ransomware-attacks-report-Microsoft> [Accessed: January 21, 2024].
18. Staff, "Time keeps on slippin' slippin' slippin': The 2023 Active Adversary Report for Tech Leaders," SCMedia, September 20, 2023. [Online]. Available: <https://www.scmagazine.com/native/time-keeps-on-slippin-slippin-slippin-the-2023-active-adversary-report-for-tech-leaders-external-remote-services> [Accessed: January 11, 2024].
19. Abbasi, S, "2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is," Qualys, December 19, 2023. [Online]. Available: <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one> [Accessed: January 9, 2024].
20. Mailk, K, "Top 10 Exploited Vulnerabilities in 2024 [Updated]," Astra, December 22, 2023. [Online]. Available: <https://www.getastra.com/blog/security-audit/top-vulnerabilities/> [Accessed: January 9, 2024].
21. Adineh, R, "A quick review on Exploiting Public-Facing Application Tactics," Medium, March 13, 2023. [Online]. Available: <https://reza-adineh.medium.com/a-quick-review-on-exploiting-public-facing-application-tactics-a3ffa4e8fa57> [Accessed: January 10, 2023].
22. Moore, P, Stanford, Z, Tripathi, S, Kharti, Y., "Weaponising VMs to bypass EDR – Akira ransomware," CyberCX, September 15, 2023. [Online]. Available: <https://cybercx.com.au/blog/akira-ransomware> [Accessed: January 14, 2024].
23. McLellan, T, Wolfram, J, Roncone, G, Lin, M, Wallace, R, Andonov, A, "Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation," Mandiant, January 17, 2024. [Online]. Available: <https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day> [Accessed: January 19, 2024].
24. Lucas, J, "Securing the cloud: Lessons learned from 2023 and what it means for 2024," Betanews, January 20, 2024. [Online]. Available: <https://betanews.com/2024/01/19/securing-the-cloud-lessons-learned-from-2023-and-what-it-means-for-2024/> [Accessed: January 21, 2024].
25. Staff, "Non-Human Access is the Path of Least Resistance: A 2023 Recap," The Hacker News, December 12, 2023. [Online]. Available: <https://thehackernews.com/2023/12/non-human-access-is-path-of-least.html> [Accessed: January 21, 2024].
26. Hill, J., "BEC and VEC Attacks on the Rise in 2023," Abnormal, August 16, 2023. [Online]. Available: <https://abnormalsecurity.com/blog/bec-vec-attacks-2023> [Accessed: January 16, 2024].
27. Mascellino, A., "Vendor Email Attacks Surged by 137% in Financial Sector in 2023," InfoSecurity, January 17, 2024. [Online]. Available: <https://www.infosecurity-magazine.com/news/vec-surged-137-financial-sector/> [Accessed: January 18, 2024].
28. Satyajit, S., "State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally," IOT Analytics, May 24, 2023. [Online]. Available: <https://iot-analytics.com/number-connected-iot-devices/> [Accessed: January 21, 2024].
29. Ghandi, V., "2023 ThreatLabz Report Indicates 400% Growth in IoT Malware Attacks," Zscaler, October 24, 2023. [Online]. Available: <https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks#united-states-attracts-the-most-malware-authors> [Accessed: January 14, 2024].

Sources

30. Staff, "Heightened DDoS Threat Posed by Mirai and Other Botnets," CISA, October 17, 2017. [Online]. Available: <https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets> [Accessed: January 15, 2024].
31. Stahie, S., "Google Mitigates Largest DDoS Attack in Its History," Bitdefender, October 13, 2023. [Online]. Available: <https://www.bitdefender.com.au/blog/hotforsecurity/google-mitigates-largest-ddos-attack-in-its-history/> [Accessed: January 15, 2024].
32. Kupchik, S., "You Had me at Hi – Mirai-Based NoaBot Makes an Appearance," Akamai, January 10, 2024. [Online]. Available: <https://www.akamai.com/blog/security-research/mirai-based-noabot-crypto-mining>. [Accessed: January 23, 2024].
33. Zak, P., "Google, Cloudflare, and AWS reported the largest DDoS attack in history," Medium, October 15, 2023. [Online]. Available: <https://medium.com/@zakpatricz/google-cloudflare-and-aws-reported-the-largest-ddos-attack-in-history-75d285b587ce>. [Accessed: January 23, 2024].
34. Toulas, B., "Medusa botnet returns as Mirai-based variant with ransomware sting," Bleeping Computer, February 7, 2023. [Online]. Available: <https://www.bleepingcomputer.com/news/security/medusa-botnet-returns-as-a-mirai-based-variant-with-ransomware-sting/>. [Accessed: 23 January 2024].
35. Heiligenstein, M., "Twitter Data Breaches: Full Timeline Through 2023," Firewall Times, October 5, 2023. [Online]. Available: <https://firewalltimes.com/twitter-data-breach-timeline/> [Accessed: January 16, 2024].
36. Powell, M., "Investigation launched into Twitter after 400m user details posted in hacking forum," Cyber Security Hub, April 1, 2023. [Online]. Available: <https://www.cshub.com/attacks/news/investigation-launched-into-twitter-after-400m-user-details-posted-on-hacking-forum> [Accessed: January 16, 2024].
37. Fung, B., "Hackers post email addresses linked to 200 million Twitter accounts, security researchers say," CNN Business, January 5, 2023. [Online]. Available: <https://edition.cnn.com/2023/01/05/tech/twitter-data-email-addresses/index.html> [Accessed: January 16, 2024].
38. Zhirinovskiy, "Discoverability by phone number/email restriction bypass," Hacker one, January 1, 2022. [Online]. Available: <https://hackerone.com/reports/1439026> [Accessed: January 19, 2024].
39. Jones, C., "The GoAnywhere data breach explained," ITPro, August 26, 2023. [Online]. Available: <https://www.itpro.com/security/data-breaches/370409/the-goanywhere-data-breach-explained> [Accessed: January 19, 2024].
40. Toulas, B., "Fortra shares findings on GoAnywhere MFT zero-day attacks," Bleeping Computer, April 19, 2023. [Online]. Available: <https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/> [Accessed: January 16, 2024].
41. Staff, "GoAnywhere MTF Vulnerability Contributes to 91% Increase in Ransomware Attacks," SOCRadar, May 3, 2023. [Online]. Available: <https://socradar.io/goanywhere-mft-vulnerability-contributes-to-91-increase-in-ransomware-attacks/>. [Accessed: January 19, 2024].
42. Sadler, D., "Data breach cost Latitude \$76 million," InformationAge, August 22, 2023. [Online]. Available: <https://ia.acs.org.au/article/2023/data-breach-cost-latitude--76-million.html> [Accessed: January 16, 2024].
43. Davidson, J., "Revealed: how hackers used a tech giant to get inside Latitude Financial," Australian Financial Review, March 24, 2023. [Online]. Available: <https://www.afr.com/technology/revealed-how-hackers-used-a-tech-giant-to-get-inside-latitude-financial-20230323-p5cukr> [Accessed: January 16, 2024].
44. Gardy, M., "Cybercrime Update 11," Latitude Financial, April 11, 2023. [Online]. Available: <https://www.latitudefinancial.com.au/about-us/media-releases/cybercrime-update-11-04-2023.html> [Accessed: January 19, 2024].
45. NCSC, "UK and allies expose Snake malware threat from Russian cyber actors," National Cyber Security Centre, May 9, 2023. [Online]. Available: <https://www.ncsc.gov.uk/news/uk-and-allies-expose-snake-malware-threat-from-russian-cyber-actors> [Accessed: January 16, 2024].
46. Skulmoski, G., "It's being called Russia's most sophisticated cyber espionage tool. What is Snake, and why is it so dangerous?" The Conversation, May 11, 2023. [Online]. Available: <https://theconversation.com/its-being-called-russias-most-sophisticated-cyber-espionage-tool-what-is-snake-and-why-is-it-so-dangerous-205405> [Accessed: January 16, 2024].
47. CISA, "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," Cybersecurity & Infrastructure Security Agency, May 24, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a> [Accessed: January 16, 2024].
48. NCSC, "MOVEit vulnerability and data extortion incident," National Cyber Security Centre, June 7, 2023. [Online]. Available: <https://www.ncsc.gov.uk/information/moveit-vulnerability> [Accessed: January 16, 2024].
49. CISA, "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34363 MOVEit Vulnerability," Cybersecurity & Infrastructure Security Agency, June 7, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a> [Accessed: January 16, 2024].
50. Newman L. & Burgess, M., "The Biggest Hack of 2023 Keeps Getting Bigger," Wired, October 2, 2023. [Online]. Available: <https://www.wired.com/story/moveit-breach-victims/>. [Accessed: January 19, 2024].
51. Staff, "Electoral Commission subject to cyber-attack," The Electoral Commission, August 8, 2023. [Online]. Available: <https://www.electoralcommission.org.uk/media-centre/electoral-commission-subject-cyber-attack> [Accessed: January 16, 2024].
52. Staff, "Electoral Commission failed basic security test before hack," BBC, September 5, 2023. [Online]. Available: <https://www.bbc.com/news/technology-66709556> [Accessed: January 16, 2024].
53. ACSC, "#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability," Australian Cyber Security Centre, November 22, 2023. [Online]. Available: <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/stopransomware-lockbit-3.0-ransomware-affiliates-exploit-cve-2023-4966-citrix-bleed-vulnerability> [Accessed: January 16, 2024].
54. Beaumont, K., "What it means – CitrixBleed ransomware group woes grow as over 60 credit unions, hospitals, financial services and more breached in US," Double Pulsar, December 4, 2023. [Online]. Available: <https://doublepulsar.com/what-it-means-citrixbleed-ransom-group-woes-grow-as-over-60-credit-unions-hospitals-47766a091d4f> [Accessed: January 16, 2024].
55. Zorz, Z., "How LockBit used Citrix Bleed to breach Boeing and other targets," Help Net Security, November 22, 2023. [Online]. Available: <https://www.helpnetsecurity.com/2023/11/22/lockbit-citrix-bleed/> [Accessed: January 16, 2024].

Sources

56. Kharpal, A, "China's ICBC, the world's biggest bank, hit by cyberattack that reportedly disrupted Treasury markets", CNBC, November 10, 2023. [Online]. Available: <https://www.cnbc.com/2023/11/10/icbc-the-worlds-biggest-bank-hit-by-ransomware-cyberattack.html> [Accessed: January 16, 2024].
57. Shen, Y., "ICBC Tells Clients to Reroute Some Trades After Cyber Issue," Bloomberg, November 10, 2023. [Online]. Available: <https://www.bloomberg.com/news/articles/2023-11-09/icbc-tells-clients-to-reroute-some-trades-amid-cyber-issue> [Accessed: January 16, 2024].
58. Fell, J., "Port operator DP world failed to fix 'critical' CitrixBleed vulnerability in IT system," ABC News, November 17, 2023. [Online]. Available: <https://www.bloomberg.com/news/articles/2023-11-09/icbc-tells-clients-to-reroute-some-trades-amid-cyber-issue> [Accessed: January 16, 2024].
59. Ainsworth, K., "DP World Australia confirms employee data was stolen during cyber attack, warns of further freight delays ahead of Christmas rush," ABC News, November 28, 2023. [Online]. Available: <https://www.abc.net.au/news/2023-11-28/dp-world-australia-employee-data-stolen-cyber-attack-freight/103161588> [Accessed: January 16, 2024].
60. Abrams, L, "How the FBI seized BlackCat (ALPHV) ransomware's servers," Bleeping Computer, December 19, 2023. [Online]. Available: <https://www.bleepingcomputer.com/news/security/how-the-fbi-seized-blackcat-alphv-ransomwares-servers/> [Accessed: January 19, 2024].
61. Newman, L.H., "A Major Ransomware Takedown Suffers a Strange Setback," Wired, December 19, 2023. [Online]. Available: <https://www.wired.com/story/alphv-blackcat-ransomware-doj-takedown/> [Accessed: January 19, 2024].
62. Staff, "APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers," CISA, April 18, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108> [Accessed: January 19, 2024].
63. Staff, "Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally," CISA, December 13, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a> [Accessed: January 19, 2024].
64. Staff, "Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns," CISA, December 07, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a> [Accessed: January 18, 2024].
65. Staff, "Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally," CISA, December 13, 2024. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a> [Accessed: January 18, 2024].
66. CISA, "#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities," CISA, February 9, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a>. [Accessed: January 18, 2024].
67. Staff, "The State of Initial Access Sales in 2023," Hadrian Threat Trends, no date. [Online]. Available: <https://hadrian.io/blog/the-state-of-initial-access-sales-in-2023>. [Accessed: January 22, 2024].
68. Matsugaya, S., "Lockbit, Blackcat, and Cl0p Preval as Top RaaS Groups", Trend Micro, September 21, 2023. [Online]. Available: <https://www.trendmicro.com/vinfo/au/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-cl0p-prevail-as-top-raas-groups-for-1h-2023>. [Accessed: January 22, 2024].
69. Rodenhauser, T. & Vignati M., "8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them," EJIL: Talk!, October 4, 2023. [Online]. Available: <https://www.ejiltalk.org/8-rules-for-civilian-hackers-during-war-and-4-obligations-for-states-to-restrain-them/>. [Accessed: January 22, 2024].
70. Antoniuk, D., "Hacktivists take sides in Israel-Palestinian war," The Record, October 11, 2023. [Online]. Available: <https://therecord.media/hacktivists-take-sides-israel-palestinian> [Accessed: January 22, 2024].
71. Margolin, H., "The Top 7 Dark Web Trends in 2023," webz.io, December 13, 2023. [Online]. Available: <https://webz.io/dwp/the-top-7-dark-web-trends-in-2023/> [Accessed: January 18, 2024].
72. Staff, "Akira," Trend Micro Research, October 5, 2023. [Online]. Available: <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/> [Accessed: January 19, 2024].
73. Arghire, I., "Dozens of Organizations Targeted by Akira Ransomware," Security Week, July 26, 2023. [Online]. Available: <https://www.securityweek.com/dozens-of-organizations-targeted-by-akira-ransomware/> [Accessed: January 19, 2024].
74. Bleih, A., "Akira Ransomware: What SOC Teams Need To Know," cyberint, November 1, 2023. [Online]. Available: <https://cyberint.com/blog/research/akira-ransomware-what-soc-teams-need-to-know/> [Accessed: January 19, 2024].
75. Greig, J., "Largest switching and terminal railroad in US investigating ransomware data theft," Recorded Future News, August 12, 2023. [Online]. Available: <https://therecord.media/belt-railway-chicago-ransomware-data-theft-akira> [Accessed: January 19, 2024].
76. Staff, "#StopRansomware: ALPHV Blackcat," CISA, December 19, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a> [Accessed: January 31, 2024].
77. Dissent, "AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC," Databreaches.net, November 15, 2023. [Online]. Available: <https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/> [Accessed: January 19, 2024].
78. Tran, D., "Russian ransomware gang AlphV targets pathology company, law firms in latest string of attacks," ABC news, September 5, 2023. [Online]. Available: <https://www.abc.net.au/news/2023-09-05/russian-ransomware-gang-alphv-targets-pathology-company-law-firm/102817900> [Accessed: January 19, 2024].
79. Greig, J., "US, Japan say 'BlackTech' Chinese govt hackers exploiting routers during attacks," The Record Media, September 28, 2023. [Online]. Available: <https://therecord.media/us-japan-say-chinese-hackers-routers>. [Accessed: January 23, 2024].
80. MITRE, "BlackTech," MITRE ATT&CK, April 6, 2022. [Online]. Available: <https://attack.mitre.org/groups/G0098/> [Accessed: January 23, 2024].

Sources

81. CISA, "People's Republic of China-Linked Cyber Actors Hide in Router Firmware," CISA, September 27, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a> [Accessed: January 23, 2024].
82. Research Team, "New Cyber Alliance: The Five Families Telegram Channel," Cyberint, September 12, 2023. [Online]. Available: <https://cyberint.com/blog/research/new-cyber-alliance-the-five-families-telegram-channel/> [Accessed: January 15, 2024].
83. Staff, "The Five Families: Hacker Collaboration Redefining the Game," SOCRadar, November 3, 2023. [Online]. Available: <https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/> [Accessed: January 19, 2024].
84. Staff, "Reflections of the Israel-Palestine Conflict on the Cyber World," SOCRadar, October 9, 2023. [Online]. Available: <https://socradar.io/reflections-of-the-israel-palestine-conflict-on-the-cyber-world/> [Accessed: January 19, 2024].
85. Subhra Dutta, T., "Five Families – Hackers Collaborate to Launch Notorious Cyber Attack," Cyber Security News, August 30, 2023. [Online]. Available: <https://cybersecuritynews.com/five-families-hackers-collaborate-cyber-attack/> [Accessed: January 19, 2024].
86. Staff, "Cybercriminals Launched "Leaksmas" Event In The dark Web Exposing Massive Volumes Of Leaked PII And Compromised Data," Resecurity, December 27, 2023. [Online]. Available: <https://www.resecurity.com/blog/article/cybercriminals-launched-leaksmas-event-in-the-dark-web-exposing-massive-volumes-of-leaked-pii-and-compromised-data> [Accessed: January 19, 2024].
87. Goldstein, G., "From Transparency to Coercion, Emerging Threat Actor Tactics," Cyberint, December 31, 2023. [Online]. Available: <https://cyberint.com/blog/thought-leadership/from-transparency-to-coercion-emerging-threat-actor-tactics/> [Accessed: January 19, 2024].
88. Nair, P., "New Malware by Lazarus-Backed Andariel Group Exploits Log4j," Bank Info Security, June 29, 2023. [Online]. Available: <https://www.bankinfosecurity.com/new-malware-by-lazarus-backed-andariel-group-exploits-log4j-a-22403> [Accessed: January 19, 2024].
89. Ilaşcu, I., "Lazarus hackers use new service to hide \$100 million in stolen crypto," Bleeping Computer, February 13, 2023. [Online]. Available: <https://www.bleepingcomputer.com/news/security/lazarus-hackers-use-new-service-to-hide-100-million-in-stolen-crypto/> [Accessed: January 19, 2024].
90. An, J., "Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in Dlang," CISCO Talos, December 11, 2023. [Online]. Available: https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/ [Accessed: January 19, 2024].
91. Staff, "LockBit Ransomware: Inside the World's Most Active Ransomware Group," Flashpoint, July 20, 2023. [Online]. Available: <https://flashpoint.io/blog/lockbit/> [Accessed: January 19, 2024].
92. Petkauskas, V., "ICBC, China's largest bank, hit with ransomware," Cybernews, November 15, 2023. [Online]. Available: <https://cybernews.com/news/industrial-commercial-bank-china-icbc-ransomware-attack/> [Accessed: December 20, 2023].
93. MITRE, "Data Encrypted for Impact," Mitre, June 16, 2022. [Online]. Available: <https://attack.mitre.org/techniques/T1486/> [Accessed: January 19, 2024].
94. MITRE, "Data from Local System," Mitre, April 1, 2022. [Online]. Available: <https://attack.mitre.org/techniques/T1533/> [Accessed: January 19, 2024].
95. Staff, "Dark Web Profile: Play Ransomware," SOCRadar, June 5, 2023. [Online]. Available: <https://socradar.io/dark-web-profile-play-ransomware/> [Accessed: January 19, 2024].
96. Staff, "An In-depth Look at Play Ransomware," Avertium, January 4, 2023. [Online]. Available: <https://explore.avertium.com/resource/an-in-depth-look-at-play-ransomware> [Accessed: January 19, 2024].
97. GitHub, "Ransomware-Play.csv," Github, January 12, 2023. [Online]. Available: [loCs/Ransomware-Play.csv at master · sophoslabs/loCs · GitHub](https://github.com/sophoslabs/loCs/blob/master/Ransomware-Play.csv) [Accessed: January 19, 2024].
98. Gatlan, S., "FBI: Play ransomware breached 300 victims, including critical orgs," Bleeping Computer, December 18, 2023. [Online]. Available: <https://www.bleepingcomputer.com/news/security/fbi-play-ransomware-breached-300-victims-including-critical-orgs/> [Accessed: January 19, 2024].
99. Staff, "Threat Actor Profile: SiegedSec," SOCRadar, October 18, 2023. [Online]. Available: <https://socradar.io/threat-actor-profile-siegedsec/> [Accessed: January 15, 2024].
100. Wikipedia, "Atlassian," Wikipedia, December 31, 2023. [Online]. Available: <https://en.wikipedia.org/wiki/Atlassian> [Accessed: January 19, 2024]. Vicens, A., "After apparent hack, data from Australian tech giant Atlassian dumped online," Cyberscoop, February 16, 2023. [Online]. Available: <https://cyberscoop.com/atlassian-hack-employee-data-seigedsec/> [Accessed: January 19, 2024].
101. Kovacs, E., "Atlassian Investigating Security Breach After Hackers Leak Data," Security Week, February 17, 2023. [Online]. Available: <https://www.securityweek.com/atlassian-investigating-security-breach-after-hackers-leak-data/> [Accessed: January 19, 2024].
102. McGraw, J.W., "GhostSec hackers target satellites to 'change the world,'" Cybernews, November 15, 2023. [Online]. Available: <https://cybernews.com/tech/ghostsec-satellite-hacking-interview/> [Accessed: January 19, 2024].
103. Ribeiro, A., "Mandiant reveals hacktivists increasingly targeting OT systems, raising likelihood of actual and even substantial OT incidents," Industrial Cyber, March 23, 2023. [Online]. Available: <https://industrialcyber.co/news/mandiant-reveals-hacktivists-increasingly-targeting-ot-systems-raising-likelihood-of-actual-and-even-substantial-ot-incidents/> [Accessed: January 19, 2024].
104. Staff, "Colombian government suffers cyberattacks by hacktivist groups," digwatch, May 29, 2023. [Online]. Available: <https://dig.watch/updates/colombian-government-suffer-cyberattacks-by-hacktivist-groups> [Accessed: January 19, 2024].
105. United States Attorney's Office, "Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service," US Department of Justice, May 9, 2023. [Online]. Available: <https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network> [Accessed: January 25, 2024].
106. Nelson, Nate, "Staff, China's Volt Typhoon APT Burrows Deeper Into US Critical Infrastructure," DarkReading, July 31, 2023. [Online]. Available: <https://www.darkreading.com/vulnerabilities-threats/china-s-volt-typhoon-apt-burrows-us-critical-infrastructure> [Accessed: December 19, 2023].
107. Tillet, A., "Five Eyes members expose China-backed hacking campaign," Australian Financial Review, May 25, 2023. [Online]. Available: <https://www.afr.com/politics/federal/five-eyes-allies-expose-details-of-volt-typhoon-hacking-campaign-20230525-p5db4d> [Accessed: January 19, 2024].

Sources

108. Antoniuk, D., "How a 'crypto drainer' tricked people into handing over \$80 million in assets worldwide," The Record, January 17, 2024. [Online]. Available: <https://therecord.media/inferno-drainer-cryptocurrency-scam-spoofing-blockchain-projects>. [Accessed: January 31, 2024].
109. Staff, "What is Anonymous Sudan?" Cloudflare, March 29 2023. [Online]. Available: <https://www.cloudflare.com/en-gb/learning/ddos/glossary/anonymous-sudan/> [Accessed: January 31 2024].
110. Seals, T, "Killnet Threatens Imminent SWIFT, World Banking Attacks," Dark Reading, June 17 2023. [Online]. Available: <https://www.darkreading.com/cyber-risk/killnet-threatens-imminent-swift-world-banking-attacks>. [Accessed: January 31, 2024].
111. Kerner, M., "Ransomware trends, statistics and facts heading into 2024," TechTarget Security, January 3, 2024. [Online]. Available: <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>. [Accessed: 29 January 2024].
112. Hay Newman, L, Burgess, M, "Ransomware Attacks Are on the Rise, Again," Wired, July 12, 2023. [Online]. Available: <https://www.wired.com/story/ransomware-attacks-rise-2023> [Accessed: January 10, 2024].
113. Alessandro Mascellino, "China Unleashes AI-Powered Image Generation For Influence Operations," Infosecurity, September 8, 2023. [Online]. Available: <https://www.infosecurity-magazine.com/news/china-ai-image-generation/#:~:text=Alessandro%20Mascellino&text=China%20has%20unveiled%20a%20new,racial%2C%20economic%20and%20ideological%20lines>. [Accessed: 12 January 2024].
114. Walter, J. "Nov 2023 Cybercrime Update | LLMs, Ransomware and Destructive Wipers Proliferate in Recent Attacks," SentinelOne, 16 November 2023. [Online]. Available: <https://www.sentinelone.com/blog/nov-2023-cybercrime-update-llms-ransomware-and-destructive-wipers-proliferate-in-recent-attacks/>. [Accessed: 17 November 2023].
115. Staff, "Vishing Attacks through Voice Cloning Using AI," Infosec Train via LinkedIn, 11 August 2023. [Online] Available: <https://www.linkedin.com/pulse/vishing-attacks-through-voice-cloning-using-ai-infosec-train>. [Accessed: 29 January 2024].

Connect with us



Adnan Amjad

Deloitte US Cyber & Strategic Leader
Partner

Deloitte & Touche LLP
aamjad@deloitte.com



Clare Mohr

Deloitte US Cyber Intelligence Lead
VP for Solution Delivery - Threat Intelligence

clmohr@deloitte.com



Kush Singh

Deloitte US Detect & Respond Leader
Principal

Deloitte & Touche LLP
kussingh@deloitte.com



William Burns

Deloitte US Cyber Detect & Respond Advisory
Managing Director Adversary Pursuit
Organization

wburns@deloitte.com



Steve Mahar

Deloitte US Client and Market Growth Leader
Managing Director

Deloitte & Touche LLP
smahar@deloitte.com



David An

Deloitte US Cyber Intelligence
Solution Delivery Manager - Risk and Financial
Advisory

davidan3@deloitte.com



Thank you.

This document contains general information only, and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.