Global Cyber Threat Intelligence (CTI)

Annual Cyberthreat Trends Report - 2024

March 2025

Table of contents

|

Executive overview | Cyberthreat trends 2024

The following report highlights overarching cyber trends and emerging issues from January 1 to December 31, 2024.

Most impactful threat actor

RansomHub

Category	Cybercriminal
Motive	Financial gain
Likelihood	Very likely
Impact	Significant

RansomHub emerged in February and operates under a ransomware-as-a-service (RaaS) model. The RansomHub threat group's differentiator is its ability to seamlessly accommodate affiliates across varying skill and experience levels [1], [2].

Most pervasive threat actor

APT29

Category	Nation state
Motive	Political gain
Likelihood	Likely
Impact	Significant

APT29 (aka. Midnight Blizzard) is a suspected nation-state cyberespionage group targeting government-related organizations globally. In 2024, the group conducted a spearphishing campaign that targeted multiple sectors.[1]

Top threat vector

Ransomware

Tactic	T1486
Likelihood	Very likely
Impact	Severe

With the emergence of over 30 new groups, ransomware remained the top threat vector for 2024. The adoption of artificial intelligence (AI) tools has led to more sophisticated attack techniques. Politically-motivated threat actors are also increasingly collaborating with RaaS operators [1].

Top trend incident response (IR) teams observed

Social engineering

Tactic	T1589
Likelihood	Likely
Impact	Severe

Deloitte's incident response (IR) teams noted that threat actors are honing their skills to exploit human behaviors as technical protections are increasingly effective. For example, threat actors are combining voice phishing (vishing) with business email compromise (BEC) attacks to steal user credentials [1].

Highlights

- Ransomware continued to be the top threat vector for the year. The RaaS model facilitates the easy creation of new groups. Affiliates are not tied to one group, making attack attribution more challenging than in previous years.
- Due to its effectiveness, social engineering continued to trend as an initial access technique for cybercriminals. The exploitation of human behavior and mistakes is again rising as technical protections are increasingly effective.
- In 2024, Deloitte CTI observed a shift from brute-force attacks to using deliberately stolen username and password combinations to authenticate on corporate virtual private networks (VPNs).
- Deloitte IR teams noted on multiple occasions that threat actors used subscription-based cloud services, shifting away from the traditionally known open-source tools that offer similar capabilities.
- Malware, particularly infostealers, remained a prominent threat as many families have developed new iterations. Despite law enforcement's takedown of Resine Stealer operations, large sample sets enable the malware to persist.

Assessments

- Deloitte CTI assesses with high confidence that threat actors will continue to leverage third-party integrations between vendors and clients. Third-party compromises can spread rapidly and can affect multiple organizations with ease.
- Deloitte CTI assesses with moderate to high confidence that social engineering, with the aid of AI, will become a top threat vector in 2025 and beyond. Technical measures to detect AI-generated content and interactions are lagging, increasingly exposing end users to this threat.
- Deloitte CTI assesses with high confidence that nation-state groups will continue to pose significant challenges to global cybersecurity efforts.

Threat vectors| Trends

Throughout 2024, Deloitte CTI observed several overarching, cross-industry threat vectors not specific to a threat actor type. This section illustrates the impact of ransomware, third-party compromises, malware trends, and Deloitte's internal underground findings.

Ransomware

Impact	Significant
Likelihood	Likely

Details

- Ransomware continued to remain a formidable threat to organizations globally. RaaS models have continued to mature, enabling less experienced and technical actors to conduct crimes.[3]
- Emerging in February 2024, RansomHub has become the most active ransomware group in 2024, having claimed over 500 victims across various sectors.[1]
- The primary method behind ransomware breaches is leveraging VPNs for initial access, with vulnerability exploitation combined with credential-based attacks to bypass multi-factor authentication requirements.[3]
- Nation-state advanced persistent threats (APTs) have been increasingly deploying ransomware by collaborating with cybercriminal groups or developing their own strains.[4]

Third-party compromise

Impact	Moderate
Likelihood	Likely

Details

- Third-party compromises increased in 2024, partly due to the use of zero-day exploits for ransomware and extortion attacks.[5]
- Third-party compromise attacks have the potential to be widespread. Data from these compromises can be leaked on dark web forums for sale.[1].

Malware trends

Impact	Significant
Likelihood	Likely

Details

- In 2024, security researchers observed new iterations of previously known malware, while law enforcement disrupted some prevalent malware families. In October, a global operation led to the takedown of RedLine Stealer. Although activity levels have decreased due to the number of RedLine samples available, malware activity persists.[6]
- LummaStealer continued to make an impact and experienced high levels of growth during the year.[6]
- One notable development is a packer-as-a-service (PaaS) dubbed "HeartCrypt" that threat actors used to protect malware by packing malicious code into legitimate binaries.[7]

Underground trends

Impact	Significant
Likelihood	Roughly even chance

Details

- The cybercriminal underground continued its rapid transformation toward decentralized, specialized, and professionally-structured operations. Due to law enforcement pressure, popular marketplaces splintered, driving activity into closed forums and encrypted channels. [1],[8],[9]
- AI became a key enabler, powering deepfake campaigns, PaaS offerings, and automated translation to target victims worldwide. Ransomware syndicates refined multi-faceted extortion tactics, while thriving initial access brokers (IABs) fueled widespread data breaches and attacks. Meanwhile, criminals embraced privacy-centric payment methods, particularly stablecoins, to evade detection.[1],[10],[11]
- Despite several high-profile takedowns, the underground community demonstrated resilience through collaboration, bulletproof hosting, and corporate-like organizational structures.[1],[8],[9],[12]

Initial access techniques | Trends

Deloitte CTI observed that the most leveraged initial access techniques in 2024 were vulnerability exploitation, social engineering, a combination of VPN exploitation with stolen passwords, and phishing. These techniques were the most impactful across all industry sectors and verticals.

Vulnerability exploitation

Impact — Severe

Likelihood — Roughly even chance

Details

- Throughout 2024, threat actors continued to exploit vulnerabilities, including zero-day vulnerabilities, to gain initial access to their victims' networks and environments.
- Large-scale ransomware groups are among the perpetrators, with Clop exploiting two zero-day vulnerabilities in December.[1]
- Notably, threat actors continued to exploit old vulnerabilities; some large-impact exploits in 2024 were over five years old. [13].

Social engineering

Impact — Severe

Likelihood — Roughly even chance

Details

- Due to its effectiveness, social engineering continues to trend as an initial access technique for cybercriminals.
- In 2024, Deloitte IR teams noted a trend in threat actors combining vishing with BEC attacks in multiple independent investigations, predominantly targeting service providers across multiple industries.
- This method involves stealing user credentials by calling the service provider's customer support to initiate a password reset for one of their clients, using a pre-registered email domain impersonating the client. One IR case revealed that the squatted domain had only been registered three days before the call, indicating this was a targeted operation [1].
- The exploitation of human behavior and mistakes was again on the rise as technical protections are increasingly effective.

Combination: VPN exploitation with stolen passwords

Impact — Severe

Likelihood — Roughly even chance

Details

- VPN exploitation remains a leading initial access vector. In 2024, Deloitte CTI observed a shift from brute-force attacks to using deliberately stolen username and password combinations to authenticate on the corporate VPN.
- Threat actors gain credentials from data breaches exposed on the dark web, IABs, or social engineering methods.
- Additionally, Deloitte IR teams noted threat actors' expanding toolsets for transversing firewalls with cloud service providers as proxies. Deloitte IR teams noted on multiple occasions that threat actors used subscription-based cloud services, shifting away from the traditionally known open-source tools that offer similar capabilities.[1]

Phishing

Impact — Sever

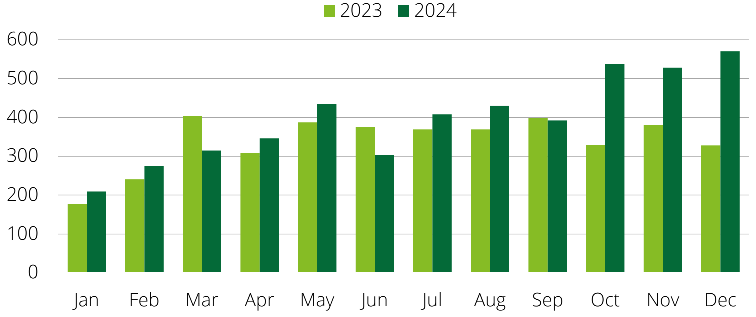
Likelihood — Almost certain

Details

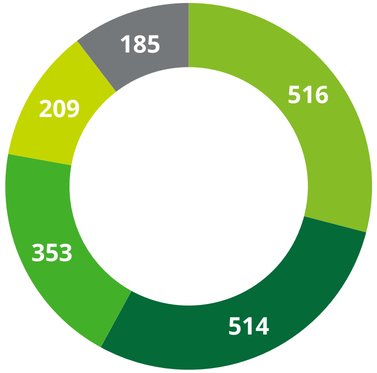
- Working with the CTI team, Deloitte's Managed Extended Detection and Response (MXDR) team observed peak phishing detections in February and May 2024, followed by a decline in detections in the third quarter, then picking up again in the fourth quarter.
- The ability of large language models (LLMs) to generate phishing content presents a significant challenge to traditional threat detection. Threat actors can generate 1,000 phishing emails in under two hours for as little as US$6.00, with LLMs likely contributing to the overall 1,265 percent increase in phishing attacks in 2024 [1].
- AI has enabled threat actors to craft highly personalized and timely phishing campaigns, enhancing their relevance and persuasiveness to their intended targets.[1]

Threat vector highlight | Ransomware

Number of attacks ransomware actors claimed responsibility for during 2023 and 2024



Top five ransomware variants observed in 2024



Ransomware trends

- Deloitte CTI observed a 17 percent increase in ransomware attack claims in 2024, peaking in the fourth quarter with 57 percent more claims compared to the fourth quarter of 2023.[1] This increase is likely due to the emergence of over 30 new ransomware groups and the increased prevalence of the RaaS model, which groups such as RansomHub utilized throughout 2024.[3]
- RansomHub, which security researchers first observed in February 2024, was the most active ransomware in 2024, with the highest number of victims listed on its leak site, followed by LockBit and Play Ransomware, who—comparatively—have both been active since early 2022.[1]
- The most common root causes for successful ransomware attacks were exploited vulnerabilities, compromised credentials, and phishing attacks.[35] Compromised credentials have traditionally been the primary initial access vector for ransomware attacks; however, the adoption of AI tools and advanced attack techniques has led to more complex and innovative attacks and methods of initial access.[14]
- The average cost of a ransomware data breach reached US$4.91 million.[15]
- Successful initiatives led by international law enforcement agencies are pressuring the ransomware ecosystem at every level. Past initiatives have involved taking down command-and-control (C2) servers, malware dropper botnets, cryptocurrency exchanges, and the arrests of key actors from notable ransomware groups.[16]

RaaS highlight

- Before 2024, the dominant groups within the ransomware landscape were the RaaS operators LockBit and ALPHV, who had been the most active groups since 2022.[A] However, the February 2024 Europol-led "Operation Cronos" resulted in the disruption of LockBit's infrastructure and an exit scam by the ALPHV group, respectively.[17].
- Security researchers estimate that two-thirds of LockBit's new victim announcements since February are duplicated or unverifiable. This activity is likely an attempt to inflate the group's perceived activity levels [3]; no activity has been seen from ALPHV since its exit scam.[1] While law enforcement activity was initially thought to have intensified distrust and signaled the collapse of the RaaS community, many smaller and more agile ransomware groups have since emerged to capitalize on the void these groups left.[2]
- Security researchers have attributed RansomHub's emergence and success in 2024 to its aggressive affiliate-friendly RaaS model. The group's affiliates have displayed diverse skills, some utilizing advanced techniques while others have relied on simpler and more accessible methods. This variety in operations showcases the group's adaptability and ability to accommodate affiliates with differing experience levels.[2]
- Other notable RaaS operations that emerged in 2024 include El Dorado/BlackLock, Lynx, Fog, and APT73/BASHE, which employ sophisticated, varied tactics, techniques, and procedures (TTPs), and have been aggressively active since their emergence.[2]
- The prevalence of the RaaS model has significantly increased the frequency, destructiveness, and complexity of ransomware operations throughout 2024. IABs continued to specialize in obtaining access to potential victims, and affiliates to focus on navigating compromised networks, payload deployment, and extortion by enabling developers to concentrate on creating and improving ransomware and its components. Aspiring cybercriminals can now specialize in different areas of RaaS operations, lowering the entry barriers for new actors and increasing the potential scale of ransomware operations in the future.[18]
- Many politically-motivated threat groups have been utilizing RaaS in their operations. Notably, the hacktivist group CyberVolk released its own RaaS platform in June 2024 and has been promoting alliances with other hacktivist groups, such as NoName057(16), and pre-emptively advertising its own politically motivated attacks, which are distinct from financially-motivated ransomware attacks.[19]

|

Threat vector highlight | Underground trends

During 2024, multinational law enforcement operations increased, resulting in significant takedowns of well-known criminal marketplaces and hosting services; however, sustained disruption continues to be challenging.

Evolving countermeasures and community resilience

Throughout 2024, multinational task forces significantly intensified their campaigns against cybercriminal operations. High-profile initiatives, including joint actions spearheaded by Interpol and other law enforcement agencies, targeted well-established dark web marketplaces such as Nemesis Marketplace and BreachForums, which are bulletproof hosting providers, and coordinated ransomware affiliates. These takedowns led to high-impact arrests, the seizure of illicit funds, the dismantling of infrastructure used for malware distribution, and the temporary takedown of LockBit because of significant law enforcement actions involving 12 countries and Eurojust. Seized domains and shuttered marketplaces disrupted criminal revenue streams, created temporary friction within underground communities-and complicated actors' ability to trade goods and services.[1],[8],[12],[20],[21]

Although these concerted efforts yielded visible results, they also underscored the persistent resilience of cybercriminal networks. Many operators seamlessly pivoted to alternative platforms or rebranded under new identities, highlighting the migratory nature of illicit communities. Furthermore, many advanced criminals adept at operational security evaded detection by migrating to invite-only forums and adopting encrypted channels, limiting the success of traditional takedowns. Consequently, law enforcement agencies increasingly partnered with private sector entities, threat intelligence providers, cybersecurity firms, and hosting companies to share real-time data and develop more comprehensive investigations.[A],[13],[9],[20].

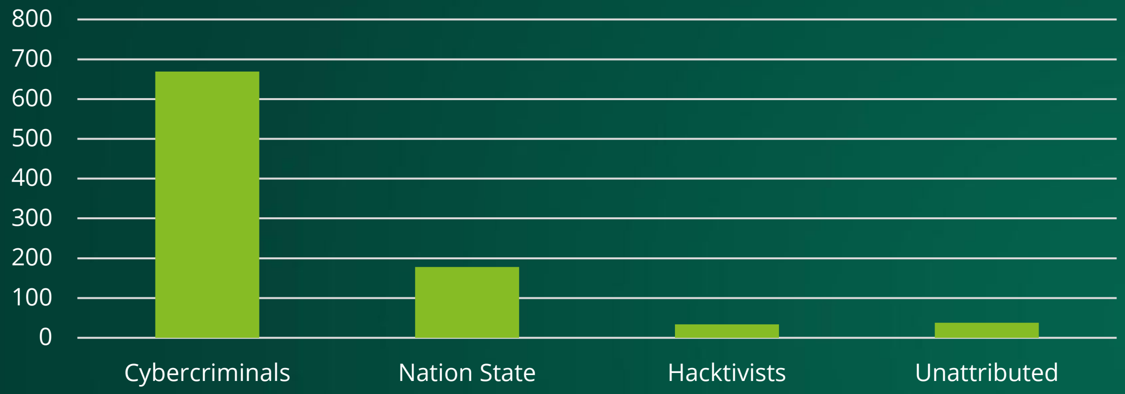
Going forward, this heightened collaboration between law enforcement and industry is expected to continue shaping future takedown strategies. Efforts such as targeting the financial conduits of cybercrime, improving cross-border legal frameworks, and bolstering digital forensic capabilities are essential to discouraging re-emergence and reducing criminal profitability; however, the cat-and-mouse dynamic remains. As authorities innovate in detection and disruption methods, cybercriminal actors likewise escalate their evasive tactics, test operational security boundaries, and thrive in the dark web's newly fragmented or hidden corners.

Implications for organizations and defenders

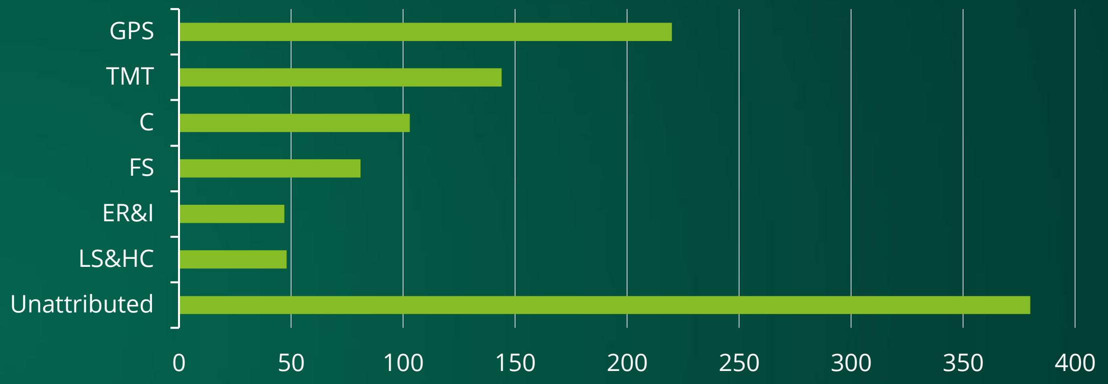
- **Temporary disruption vs. ongoing adaptation:** While takedowns impede criminal marketplaces, threat actors often reconstitute quickly, indicating a continual need for intelligence-driven defense.[1],[22]
- **The value of collaboration:** Closer public-private teaming and information-sharing initiatives are essential in forging a broad picture of the threat landscape.[1],[8],[22]
- **Preparedness and agility:** Organizations should maintain robust monitoring of new or emerging dark web venues, so they can adapt their defensive strategies when criminals relocate or evolve their operations.[9],[11]

Summary of data

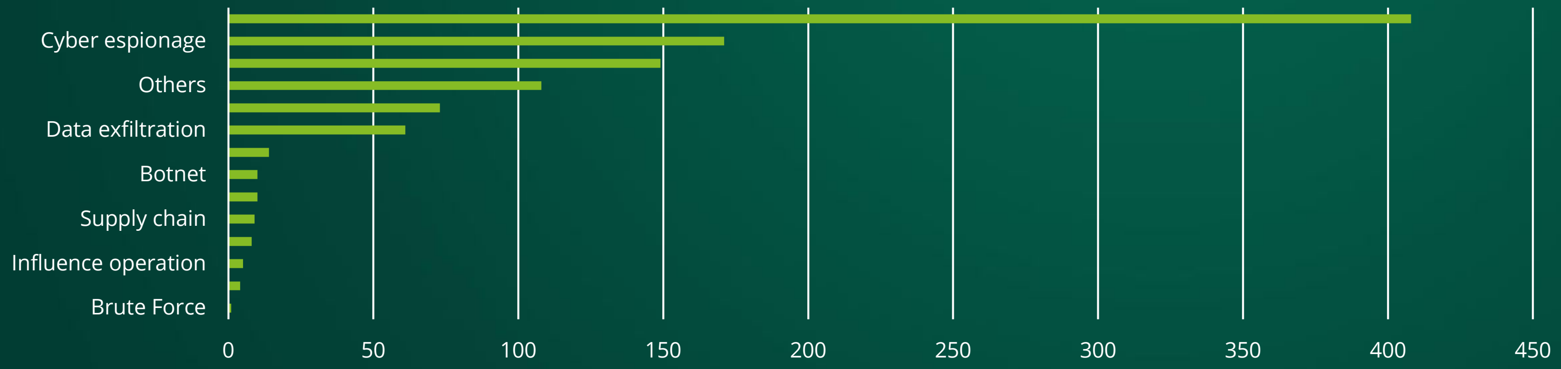
The Deloitte CTI performs internal threat research and gathers open-source intelligence, including cyber events from forums and news media dedicated to cyberthreat activities. The data in this section summarizes observed activity between January and December 2024.



Cyber events observed by threat actor type



Cyber events observed targeting specific industries



Cyber events observed by type

Industry	Key
GPS	Government & Public Services
TMT	Technology, Media & Telecommunications
C	**Consumer**
FS	Financial Services
ER&I	Energy, Resources & Industrials
LS&HC	Life Sciences & Health Care

Threat actors |Overview

	Motivation	Likelihood	Top Actors
Nation-state linked	Political, espionage, and financial	Likely, significant long-term impact	APT29, Salt Typhoon, and Volt Typhoon
Cybercriminals	Financial	Likely, significant immediate impact	Clop, LockBit, and RansomHub
Hacktivists	Political	Roughly even chance, Moderate impact	CyberVolk and NoName057(16)
Insider threats	Financial, revenge, fear (e.g., blackmail)	**Malicious:** Roughly even chance, severe impact **Unintentional:** Likely, significant impact	Not applicable

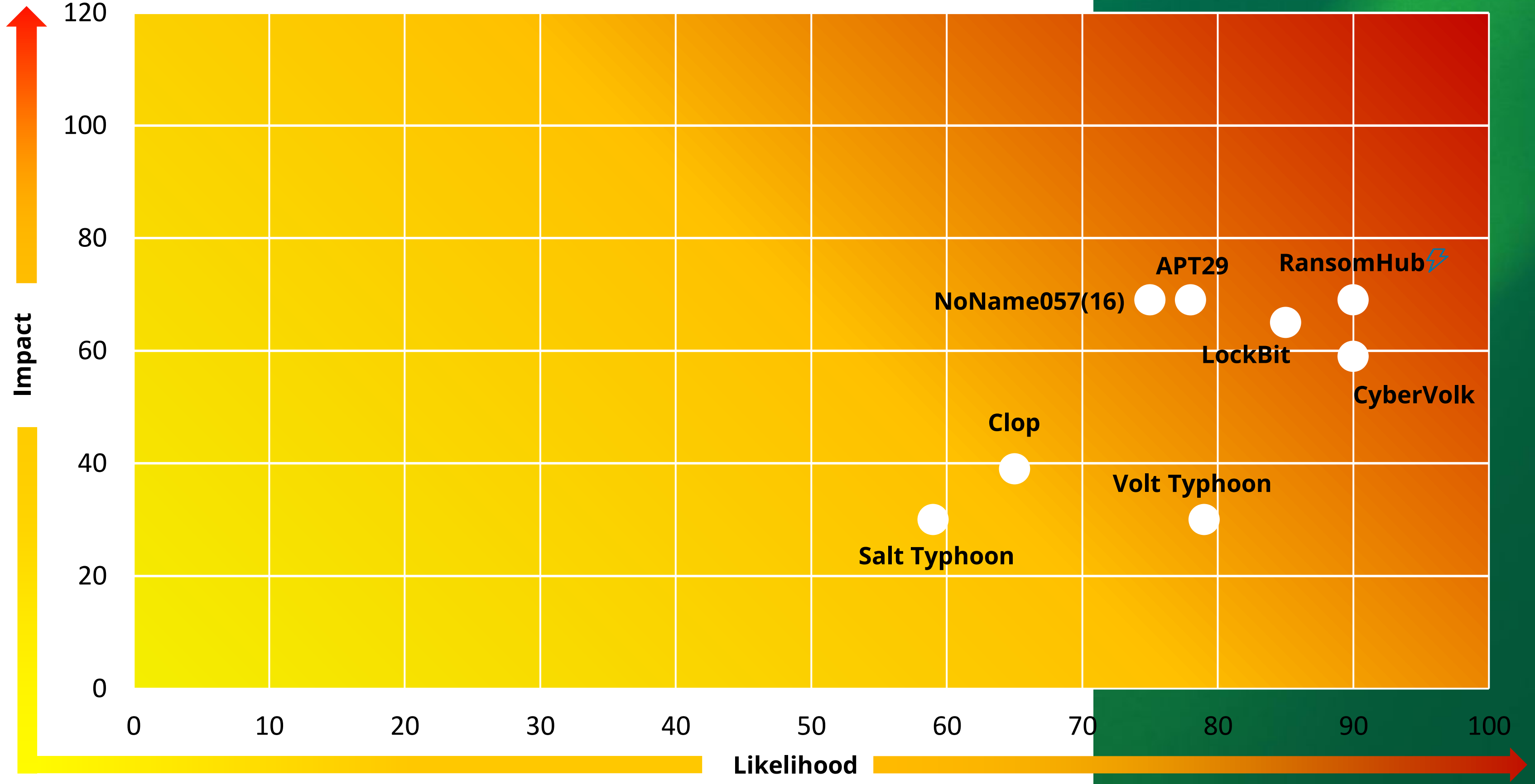
- In 2024, nation-state-linked cyber actors intensified their operations, focusing on espionage and intelligence gathering.
- APT29, aka Cozy Bear, continued its sophisticated cyber-espionage campaigns targeting governmental and non-governmental organizations globally.
- Salt Typhoon conducted extensive cyber-espionage campaigns globally, particularly against North American targets.
- Volt Typhoon was active in cyber operations. This group employed advanced techniques to infiltrate networks, exfiltrate sensitive data, and monitor communications, which posed significant challenges to global cybersecurity efforts.[23]

- The aggressive activities of ransomware groups marked the cybercriminal landscape in 2024.
- Clop, a ransomware group, was responsible for several high-profile attacks, including those exploiting zero-day vulnerabilities.
- LockBit maintained its position as a dominant ransomware operator in spite of the earlier takedown, executing numerous attacks across various sectors.
- RansomHub emerged as a notable player, facilitating numerous attacks by offering RaaS, enabling less skilled actors to launch sophisticated cyber-extortion campaigns.[24]

- Hacktivist activities in 2024 leveraged cyberattacks to advance political narratives and influence public opinion.
- CyberVolk, a politically-motivated group, targeted entities perceived as adversaries by engaging in website defacements and data leaks to promote its agenda.
- NoName057(16), another hacktivist group, conducted distributed denial of service (DDoS) attacks against government and media websites in countries supporting European nation-states, aiming to disrupt operations and spread propaganda.[19]

- During 2024, insider threats remained a significant concern for organizations.
- While specific actors are not named, many incidents involved employees exploiting their access to sensitive information for personal gain or corporate espionage.
- These threats often resulted in data breaches, financial losses, and reputational damage. Organizations continue to face challenges in detecting and mitigating insider threats due to the trusted status of these individuals within the company.[25]

Threat actors | Trending and emerging in 2024



⚡Re/Emerging Threat Actors

This image highlights the most trending and impactful threat actors throughout 2024 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.

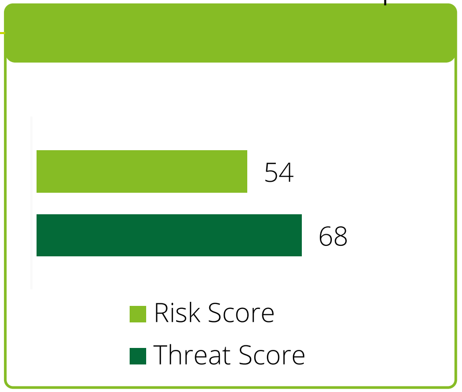
"Emerging" means the threat actor has begun activity in early 2024. "Re-emerging" means that the threat actors have been inactive for more than six months prior to the reporting period and have recently become active again.

|

Threat actor profiles | Trending and emerging

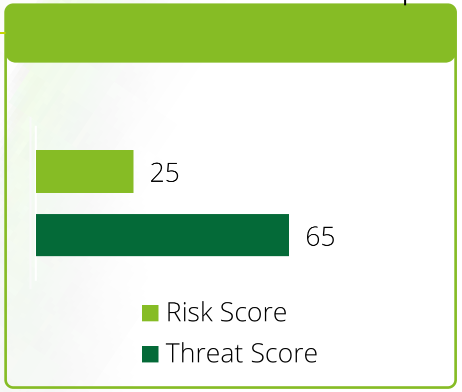
APT29

Category	Nation state
Motive	Political gain
Likelihood	Likely
Impact	Significant



Clop

Category	Cybercriminal
Motive	Financial gain
Likelihood	Likely
Impact	Moderate



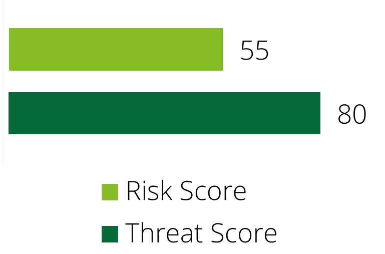
- APT29, also known as Midnight Blizzard, is a suspected nation state-sponsored cyber-espionage group with links to intelligence services and has been active since at least 2008. Security researchers have observed the group employing a variety of toolsets, most of which were custom-built and featured in highly targeted campaigns. The group targets government-related organizations in the Asia-Pacific region, Europe, and North America.[1]
- The group leverages open-source tools, including Mimikatz and PsExec. The group also utilizes cryptography and anti-detection techniques such as steganography in its toolsets, highlighting a higher level of sophistication, as these are typically used for evading analysis and investigation.[1]
- In 2024, the group conducted a spearphishing campaign that targeted education, defense, government, and private sector organizations in multiple countries. These phishing emails utilized malicious network communication protocol configuration files that contained several sensitive settings that would result in significant information exposure.[1]

- Clop is a ransomware group that operates under the RaaS scheme and has been active since at least February 2019. The group is financially-motivated and security researchers believe the threat actor TA505 operated the ransomware.[1]
- Clop predominantly uses phishing emails to gain initial access and has also been seen exploiting numerous zero-day vulnerabilities.
- The group mainly targets the financial, industrial, technology sectors, and health care sectors.[1]
- Clop manages its own data leak site (DLS), "CL0P^_-LEAKS," which is accessible via Tor and is known to issue high ransom demands that can escalate to tens of millions of dollars.[1]
- In December 2024, the group was observed exploiting two zero-day vulnerabilities [1].

Threat actor profiles | Trending and emerging

CyberVolk

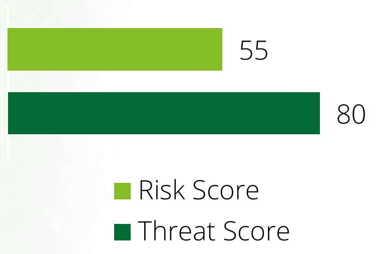
Category	Hacktivist
Motive	Political gain
Likelihood	Very likely
Impact	Significant



- Established in March 2024 and officially active since July 1, CyberVolk is an Asia-based hacktivist group aligned with a politically-motivated APT organization that includes groups such as NoName057(16) and Killnet.[26]
- CyberVolk employs a variety of ransomware builders, such as AzzaSec, Diamond, LockBit, and Chaos, demonstrating adaptability and posing challenges for tracking.[19]
- The group targets political entities opposing nation-state interests and engages in activities like website defacements and data leaks to advance its agenda.[19]
- A loose collective of mostly low-skilled actors, CyberVolk absorbs and adapts a wide array of destructive malware for use against political targets.[19]

LockBit

Category	Cybercriminal
Motive	Financial gain
Likelihood	Very likely
Impact	Significant



- LockBit is a ransomware threat group that security researchers first observed in 2019.[1] The group operates in a RaaS model, recruiting affiliates in return for a fraction of the ransom obtained from each attack (up to 80 percent).
- The group targets organizations operating in various sectors, including global commercial, communications, financial services, and retail worldwide, primarily focusing on the Asia-Pacific, European, and North American regions.
- LockBit continues to update its TTPs and toolset, which accounts for its long-standing presence in the ransomware landscape. It has been noted that the group's TTPs overlap with other ransomware groups because many of its affiliates are simultaneously involved in other RaaS operations.[1]
- The group gains initial access through various means, such as purchasing it from IABs, social engineering, or brute-force attacks. LockBit also uses a double-extortion strategy in which the threat group steals data from the network before encrypting devices.[27]
- Despite law enforcement interference in February 2024, the group continued to target victims throughout 2024. The group's scores remain high due to continued detections.

Threat actor profiles | Trending and emerging

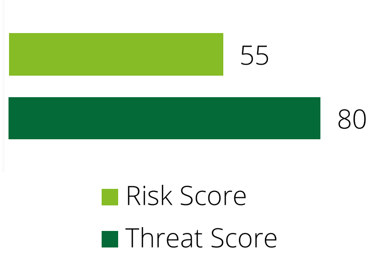
NoName057(16)

Category — Hacktivist

Motive — Political gain

Likelihood — Very likely

Impact — Significant



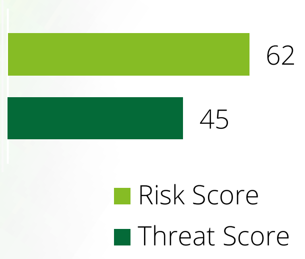
RansomHub

Category — Cybercriminal

Motive — Financial gain

Likelihood — Very likely

Impact — Significant



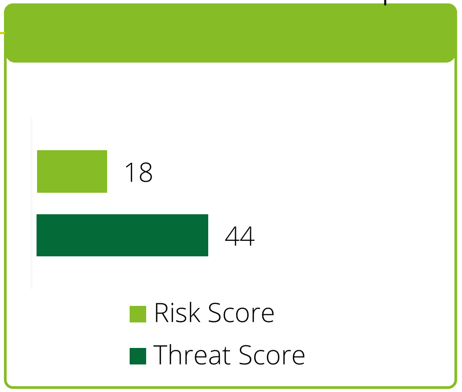
- NoName057(16) is a hacktivist collective operating in alignment with a nation-state, conducting cyberattacks against entities perceived as adversaries to national political interests.[28]
- The group relies heavily on HTTPS application-layer DDoS attacks, often sourcing attacks from the same infrastructure and targeting similar countries and industries.[29]
- In September 2024, NoName057(16), along with other politically-motivated threat actors, launched DDoS attacks on East Asian targets for political reasons.[30]
- Noname057(16) utilizes the custom crowdsource botnet named "DDOSIA," leveraging politically motivated hacktivists willing to download and install a bot on their computers, which the group then uses in DDoS attacks. DDOSIA also gives financial incentives to the top contributors for successful attacks, maximizing the available botnet size.[30]

- RansomHub is a financially motivated threat group that emerged in February 2024 and operates under a RaaS model. The group previously stated that its program's affiliates could initially receive the ransom payment on their cryptocurrency wallets and then transfer the agreed-upon cut to the ransomware operator (allegedly 10 percent).[1]
- The group has targeted organizations worldwide, with most victims registered across the Americas. Security researchers have observed the threat group targeting organizations mainly in the construction, financial services, retail, and technology sectors.[1]
- RansomHub manages its own DLS, which lists the victims it compromises and typically lists the kinds of data exfiltrated. It also includes a countdown indicating when the group will make the information public if no ransom payment is received.[1] The group resembles several Eastern European ransomware groups.[1]
- Security researchers dubbed RansomHub as one of the most prominent ransomware groups, claiming over 500 victims across various sectors in 2024.[31],[1]

Threat actor profiles | Trending and emerging

Salt Typhoon

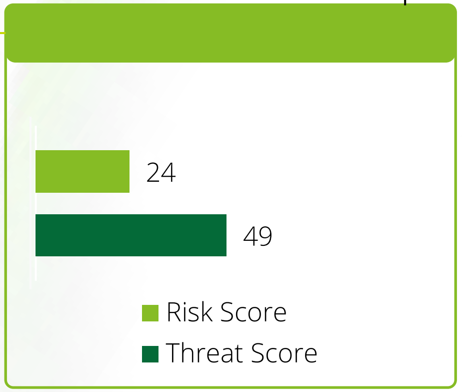
Category	Nation state
Motive	Cyber espionage
Likelihood	Likely
Impact	Moderate*



- Salt Typhoon is a nation-state threat group that has conducted espionage operations since at least 2019. The group typically targets government organizations and companies in the telecommunications industry; however, engineering companies, hospitality organizations, and law firms have also been affected.[1]
- Typically, Salt Typhoon distributes a custom backdoor known as "SparrowDoor"; however, its new backdoor, "GhostSpider," was observed in 2024.
- In 2024, US law enforcement agencies confirmed that the group had breached networks at multiple telecommunications companies to steal the call data of prominent political figures.[32] It was attributed to another cyber-espionage campaign targeting Southeast Asian telecommunication companies to Salt Typhoon by, where the group deployed the GhostSpider backdoor.[33]
- As of December 2024, US law enforcement agencies conducted investigations that noted that the full scope of the breaches had not yet been determined, and recovery efforts were expected to take years.[1]

Volt Typhoon

Category	Nation state
Motive	Cyber espionage
Likelihood	Likely
Impact	Moderate*



- Volt Typhoon is a nation-state threat actor first observed in mid-2021. The threat group performs cyber-espionage campaigns primarily targeting the Asia-Pacific region and Americas, impacting organizations in the communications, construction, education, government, manufacturing, maritime, technology, transportation, and utilities sectors.[1]
- Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber-espionage or intelligence-gathering operations; of note, US agencies warned cybersecurity defenders that Volt Typhoon has been pre-positioning themselves on US critical infrastructure organizations' networks to enable disruption or destruction of critical.[34]
- Volt Typhoon stands out for attacks against infrastructure-specific targets such as power grids and water supply systems, and stealthy C2 operations such as managing and controlling the targeted infrastructure using living-off-the-land techniques.
- Volt Typhoon frequently exploits known vulnerabilities in and using valid stolen credentials for initial access and persistence. The group also uses open-source and administration tools such as Mimikatz and Ntdsutil to extract credentials. Volt Typhoon maintains persistence via compromised VPN servers and system-on-a-chip devices.[34]

*Note: The tangible impact of these threat actors depends on the global geopolitical context at a given time. If an event is averse to the sponsoring entity of these actors, the impact rating assessment will increase accordingly.

|

Sourcing statement

Tradecraft: Deloitte CTI applies the Intelligence Community Directive 203 Analytic Standards to its products and reports— as well as other intelligence community-based tradecraft such as combating biases, techniques—for analysis (e.g., alternatives, competing hypothesis) and sourcing disclosures.

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

Collection: Deloitte CTI combines its proprietary collection with subscriptions to achieve 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. Melnyk, S., "The New Face of Ransomware: Key Players and Emerging Tactics of 2024," Trustwave, 21 January 2025. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-new-face-of-ransomware-key-players-and-emerging-tactics-of-2024/. [Accessed: 22 January 2025].
3. Alamri, A.H., "Dragos Industrial Ransomware Analysis: Q3 2024," Dragos, 17 December 2024. [Online]. Available: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2024/. [Accessed: 19 December 2024].
4. Muncaster, P., "APT groups are increasingly deploying ransomware – and that's bad news for everyone," WeLiveSecurity, 07 January 2025. [Online]. https://www.welivesecurity.com/en/business-security/state-aligned-apt-groups-increasingly-deploying-ransomware/. [Accessed: 13 January 2025].
5. Staff, "2024 Data Breach Investigations Report," Verizon, 2024. [Online]. Available: https://www.verizon.com/business/en-au/resources/reports/dbir/. [Accessed: 16 December 2024].
6. Kropac, J., "ESET Threat Report H2 2024," WeLiveSecurity, 16 December 2024. [Online]. Available: https://www.welivesecurity.com/en/eset-research/eset-threat-report-h2-2024/. [Accessed: 17 December 2024].
7. Tujague, J., & Bunce, D., "Crypted Hearts: Exposing the HeartCrypt Packer-as-a-Service Operation," Unit 42, 13 December 2024. [Online]. Available: https://unit42.paloaltonetworks.com/packer-as-a-service-heartcrypt-malware/. [Accessed: 17 December 2024].
8. Searchlight Cyber Analysts, "Three Notable Dark Web Law Enforcement Takedowns of 2024 So Far," Searchlight Cyber, 03 June 2024. [Online]. Available: https://slcyber.io/three-notable-dark-web-law-enforcement-takedowns-of-2024-so-far/. [Accessed: 23 January 2025].
9. Mcpherson, P., & Wilson, T., "Telegram app hosts 'underground markets' for Southeast Asian crime gangs, UN says," Reuters, 08 October 2024. [Online] Available: https://www.reuters.com/world/asia-pacific/criminal-networks-southeast-asia-flourish-telegrams-underground-markets-un-says-2024-10-07/. [Accessed: 23 January 2025].
10. Burgess, M., & Hay Newman, L., "Pig Butchering Scams Are Going High Tech," Wired, 12 October 2024. [Online]. Available: https://www.wired.com/story/pig-butchering-scams-go-high-tech/. [Accessed: 23 January 2025].
11. Lin, Z., & Cui, J., & Liao, X., & Wang, X., "Malla: Demystifying Real-world Large Language Model Integrated Malicious Services," arXiv, 19 August 2024. [Online]. Available: https://arxiv.org/abs/2401.03315. [Accessed: 23 January 2025].
12. Staff, "Bulletproof Hosting: A Critical Cybercriminal Service," Intel471, 22 January 2024. [Online]. Available: https://intel471.com/blog/bulletproof-hosting-a-critical-cybercriminal-service. [Accessed: 23 January 2025].
13. Staff, "2024 Threat Landscape Statistics: Ransomware Activity, Vulnerability Exploits, and Attack Trends," Rapid7, 16 December 2024. [Online]. Available: https://www.rapid7.com/blog/post/2024/12/16/2024-threat-landscape-statistics-ransomware-activity-vulnerability-exploits-and-attack-trends/. [Accessed: 13 January 2025].
14. Staff, "Ransomware in 2024: Latest Trends, Mounting Threats, and the Government Response," TRM Labs, 11 October 2024. [Online]. Available: https://www.trmlabs.com/post/ransomware-in-2024-latest-trends-mounting-threats-and-the-government-response. [Accessed: 21 January 2025].
15. Staff, "Cost of a Data Breach Report 2024," IBM, 30 July 2024. [Online]. Available: https://www.ibm.com/reports/data-breach. [Accessed: 21 January 2025].
16. Staff, "Largest ever operation against botnets hits dropper malware ecosystem," Europol, 30 May 2024. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem. [Accessed: 11 December 2024].
17. Staff, "Law enforcement disrupt world's biggest ransomware operation," Europol, 20 February 2024. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation. [Accessed: 11 December 2024].
18. Watson, M., "Ransomware report reveals evolving threat landscape in 2024," Security Brief, 18 December 2024. [Online]. Available: https://securitybrief.com.au/story/ransomware-report-reveals-evolving-threat-landscape-in-2024. [Accessed: 22 January 2025].
19. Walter, J., "CyberVolk | A Deep Dive into the Hacktivists, Tools and Ransomware Fueling Pro-Russian Cyber Attacks," Sentinel Labs, 25 November 2024. [Online]. Available: https://www.sentinelone.com/labs/cybervolk-a-deep-dive-into-the-hacktivists-tools-and-ransomware-fueling-pro-russian-cyber-attacks/. [Accessed: 28 January 2025]
20. Johnson, A., & Thies, B., "Cybercrime News & Analysis to Close Out the Year," SpyCloud Labs, 03 December 2024. [Online]. Available: https://spycloud.com/blog/2024-cybercrime-update-and-2025-predictions/. [Accessed: 20 January 2025].

Sources

21. "LockBit power cut: four new arrests and financial sanctions against affiliates," Europol, 02 October 2024. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates. [Accessed: 20 January 2025].
22. Goodchild, J., "What Security Lessons Did We Learn in 2024?," DarkReading, 31 December 2024. [Online]. Available: https://www.darkreading.com/cyber-risk/security-lessons-learn-2024. [Accessed: 20 January 2025].
23. Caveza, S., "Salt Typhoon: An Analysis of Vulnerabilities Exploited by this State-Sponsored Actor," Tenable, 23 January 2025. [Online]. Available: https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor. [Accessed: 29 January 2025].
24. De Oliveira, A., "Ransomware: biggest groups responsible for attacks in 2024," Lumiun, 03 October 2024. [Online]. Available: https://www.lumiun.com/blog/en/ransomware-largest-groups-responsible-for-2024-attacks. [Accessed: 29 January 2025].
25. Nadeau, J., "83 Percent of organizations reported insider attacks in 2024," SecurityIntelligence, 26 November 2024. [Online]. Available: https://securityintelligence.com/articles/83-percent-organizations-reported-insider-threats-2024. [Accessed: 29 January 2025].
26. Berg, J., & Donyina, F., "Cyber Threat Awareness Report: Emerging Threats from CyberVolk and Qilin Ransomware – October 04, 2024," CVP, 04 October 2024. [Online]. Available: https://www.cvpcorp.com/cyber-blog/cyber-threat-awareness-report-october-4-2024. [Accessed: 03 February 2025].
27. Staff, "Understanding Ransomware Threat Actors: LockBit," CISA, 14 June 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a. [Accessed: 26 November 2024].
28. Watt, C., "Threat Intelligence NoName057(16) Threat Actor Profile," Quorum Cyber, 18 April 2024. [Online]. Available: https://www.quorumcyber.com/threat-actors/noname057-threat-actor-profile. [Accessed: 03 February 2025].
29. Nawrocki, M., & Conrad, C., & Arenberg, C., "NoName057(16) Campaign Analysis," NETSCOUT, 16 January 2024. [Online]. Available: https://www.netscout.com/blog/asert/noname057-16. [Accessed: 03 February 2025].
30. "Pro-Russian Hacktivists Target Organizations in Taiwan With DDoS Attack Campaign," Radware, 13 September 2024. [Online]. Available: https://radware.com/security/threat-advisories-and-attack-reports/pro-russian-hacktivists-target-organizations-in-taiwan-with-ddos-attack-campaign. [Accessed: 03 February 2025].
31. Mahendru, P. "The State of Ransomware in Financial Services 2024," Sophos News, 24 June 2024. [Online]. Available: https://news.sophos.com/en-us/2024/06/24/the-state-of-ransomware-in-financial-services-2024/. [Accessed: 30 September 2024].
32. Grieg, J., "US agencies confirm Beijing-linked telecom breach involving call records of politicians, wiretaps," The Record, 14 November 2024. [Online]. Available: https://therecord.media/us-agencies-confirm-china-telecom-hack-wiretaps. [Accessed: 12 December 2024].
33. Chang, L M., Chen, T., Barmejo, L. and Lee, T., "Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions," Trend Micro, 25 November 2024. [Online]. Available: https://www.trendmicro.com/en_us/research/24/k/earth-estries.html. [Accessed: 24 January 2025].
34. Staff, "PRC State-sponsored cyber activity: Actions for critical infrastructure leaders," Australian Signals Directorate, March 2024. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2024-03/Fact_Sheet_for_Leaders_Volt_Typhoon_03202024.pdf. [Accessed: 25 November 2024].

Clare Mohr
Deloitte US Cyber Threat Intelligence
Vice President of Solution Delivery
Deloitte & Touche LLP

Shawn Cozzolino
Deloitte US Cyber Threat Intelligence
Senior Solution Delivery Manager
Deloitte & Touche LLP

David An
Deloitte US Cyber Threat Intelligence
Solution Delivery Manager
Deloitte & Touche LLP

Will Burns
Deloitte US Detect & Respond
Managing Director
Deloitte & Touche LLP

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation 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 presentation.

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