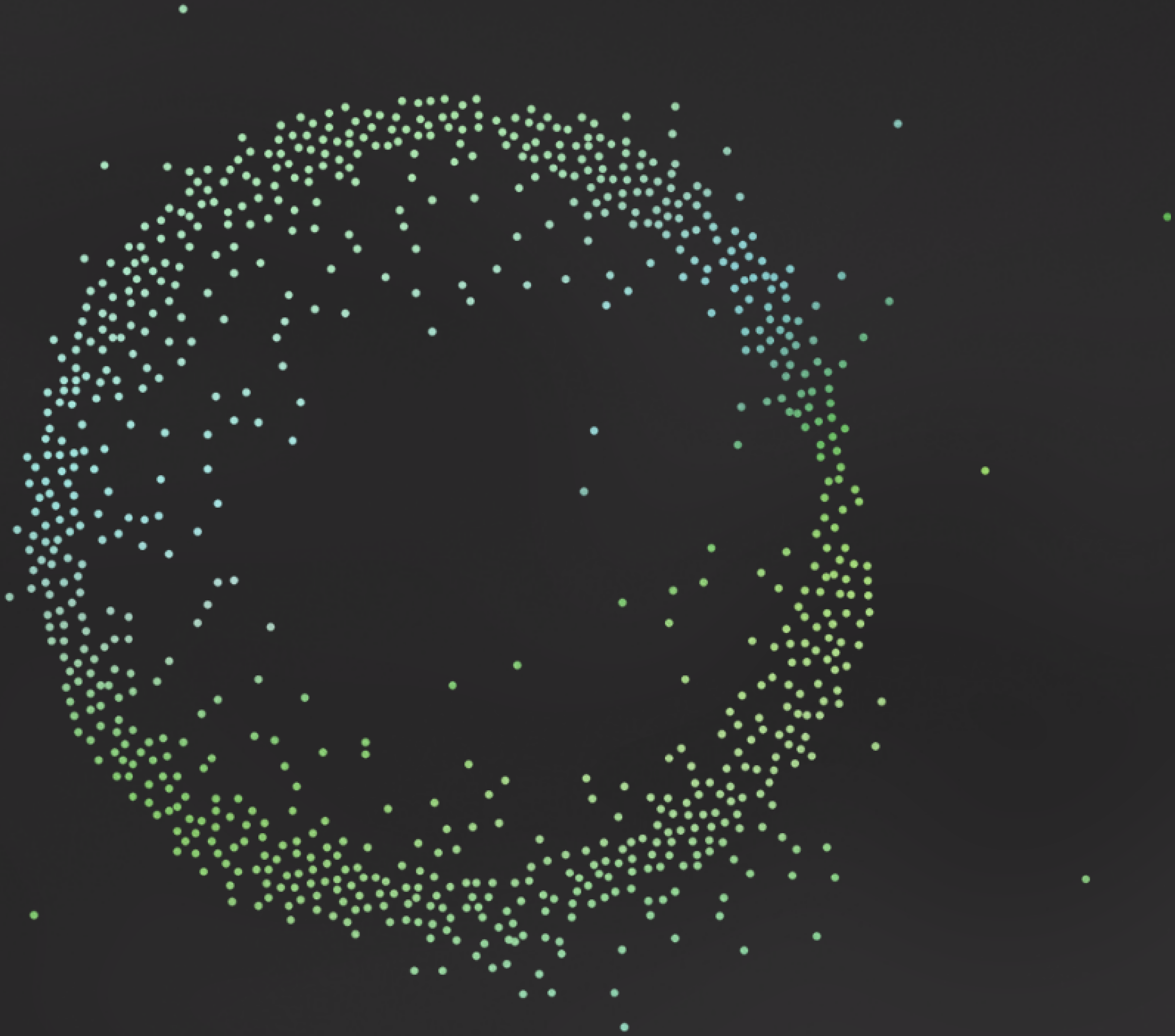
Deloitte.



Global Cyber Threat Intelligence (CTI)

Mid-year cyber threat trends 2025

Publish date: September 2025

Table of contents

01 **Executive overview**

High-level presentation of top threat actors, threat vectors, incidents, and overall assessment

02 **Cross-industry threat vectors**

Trending and emerging high-level threat vectors with a global impact

03 **Notable cybersecurity events**

Timeline of the top notable cybersecurity events globally between January – June 2025

04 **Threat vector highlights**

Spotlight on the underground, ransomware, and malware threat landscape

05 **Threat actors**

High-level overview of categories, heatmap, and trending and emerging threat actors with a global impact

Executive overview | Mid-year cyber threat trends 2025

The following report highlights overarching cyber trends and emerging issues from January 1, 2025, to June 30, 2025.

Most impactful threat actor

APT28

Category	Nation-state
Motive	Political and financial gain
Likelihood	Almost certain
Impact	Severe

APT28 is noted as the most impactful due to its cyber espionage campaigns against geopolitical targets. These are primarily conducted via reusing and redefining its toolset in response to defensive measures by intelligence agencies [1] [2].

Most trending threat actor

Qilin

Category	Cybercriminal
Motive	Financial gain
Likelihood	Likely
Impact	Significant

For the first half of 2025, Deloitte CTI highlighted Qilin (formerly Agenda) as the most trending due to its uptick in activity since April. The group operates as a Ransomware-as-a-Service (RaaS) operation and are opportunistic [1] [3].

Top threat vector

Ransomware

Tactic	TA0040
Likelihood	High
Impact	Probable

Ransomware continues as a prevalent threat, with there being a noticeable shift in groups due to changing of affiliate loyalty and the emergence of new groups [4].

Top industry targeted

Government and Public Services (GPS)

Motive	Espionage and Intellectual Property gain

In the first half of 2025, GPS was noted as the top targeted industry. This industry is targeted by nation-states and cybercriminals alike due to the possession of sensitive information [1].

Highlights

- **Ransomware**: **Outages among ransomware groups like 8Base and RansomHub**, particularly the latter's March to April disruption, led to a drop in attacks, **while groups like Qilin saw a surge**, likely due to migrating affiliates [5] [3].
- **Artificial intelligence (AI)**: There's a growing use of AI in cybercrime. This is evident in the creation of WormGPT (an uncensored large language model (LLM) tool) and its spin-offs and convincing deepfake videos, with researchers highlighting the potential of Generative AI tools to dramatically alter the cybersecurity landscape [6].
- **Infostealers**: Lumma, StealC, and Vidar have advanced significantly, showcasing sophisticated tactics such as fake CAPTCHAs, expanded payload delivery, and disguised as trusted tools to evade detection and steal sensitive data [7] [8] [9].

Assessments

- Deloitte CTI assesses with high confidence that new ransomware groups will continue to emerge in the second half of 2025, aiming to exploit the vacuum left by weakened or offline operations by recruiting displaced affiliates and repurposing leaked builder kits and infrastructure.
- Deloitte CTI assesses with medium confidence that threat actors will increasingly combine infostealers and ransomware loaders into hybrid campaigns, allowing them to first exfiltrate sensitive data and then encrypt systems, maximizing extortion leverage.
- Deloitte CTI assesses with medium confidence that infostealer variants such as Lumma Stealer and StealC will drive a surge in credential harvesting operations, particularly as these tools become more modular and accessible through cybercrime marketplaces.

Mid-year cyber threat trends 2025

Cross-industry threat vectors | Trends

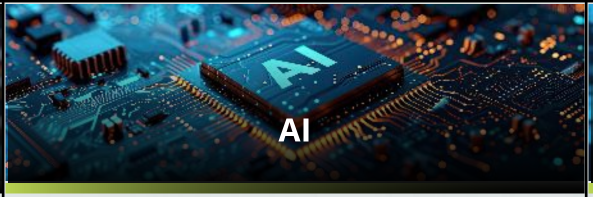
During the first half of 2025, Deloitte CTI observed several overarching, cross-industry threat vectors, not specific to threat actor type. This slide illustrates the global impact of ransomware, malicious AI use cases, globally trending malware, and our observations from underground forums and marketplaces.

Ransomware

Impact	High
Likelihood	Probable

Details

- Numerous ransomware groups including 8Base and RansomHub experienced outages in 2025. In particular, RansomHub's outage began in the end of March and continued into April. This in turn led to a significant decrease in attacks from prior months [3] [5].
- On the other hand, there has been an increase in activity by other ransomware groups, where it's believed that affiliates have been migrating. One case is Qilin, who experienced a 48 percent increase from March to April, and this is suspected due to the shift of RansomHub affiliates to this group [3] [10].
- In recent months, new ransomware groups continue to emerge, with many having listed multiple organizations on their data leak sites (DLS) in short periods of time [1].



AI

Impact	Moderate
Likelihood	Roughly even chance

Details

- AI continues to be utilized by threat groups and cybercriminals in cyber attacks and to assist in making attacks more accessible for those who are less skilled.
- Despite the shutting down of WormGPT in 2023, cybercriminals continue to use variants of it in 2025. One of these was released in February and it is powered by two different open-source AI tools [6].
- Recent reports also highlight that cybercriminals are leveraging AI to create deepfake videos that are impersonating victims [1].
- Researchers expected that agentic AI will redefine the cybersecurity landscape, since it can be utilized by defenders and attackers alike [11] [12].

Malware trends

Impact	Significant
Likelihood	Likely

Details

- In 2025, malware continues to evolve with new versions and completely new malware appearing on a regular basis. One example is ResolverRAT, a remote access trojan (RAT) with layered evasion techniques and advanced in-memory execution. It has observed similarities to Rhadamanthys and Lumma Stealer [13].
- The use of malware typically available to low-level cyber criminals are now regularly being utilized in layered and obfuscated attacks, highlighting the combination of commodity tools with advanced tactics [14].

Underground trends

Impact	Moderate
Likelihood	Roughly even chance

Details

- In the first half of 2025, cybercriminals continue to advertise the sale of data and access to companies across the globe. Breached forums were noted as being among of the most active. Organizations from the US were listed the most and GPS was the most listed industry [1].
- Another user on a foreign language underground forum dubbed "blink" was observed being quite active in January and February, and listed access to ten different organizations across multiple global regions. These were all listed for auction with various starting prices, with the highest being USD $2,000 and contained a blitz price of $4,000 for quicker sale [1].

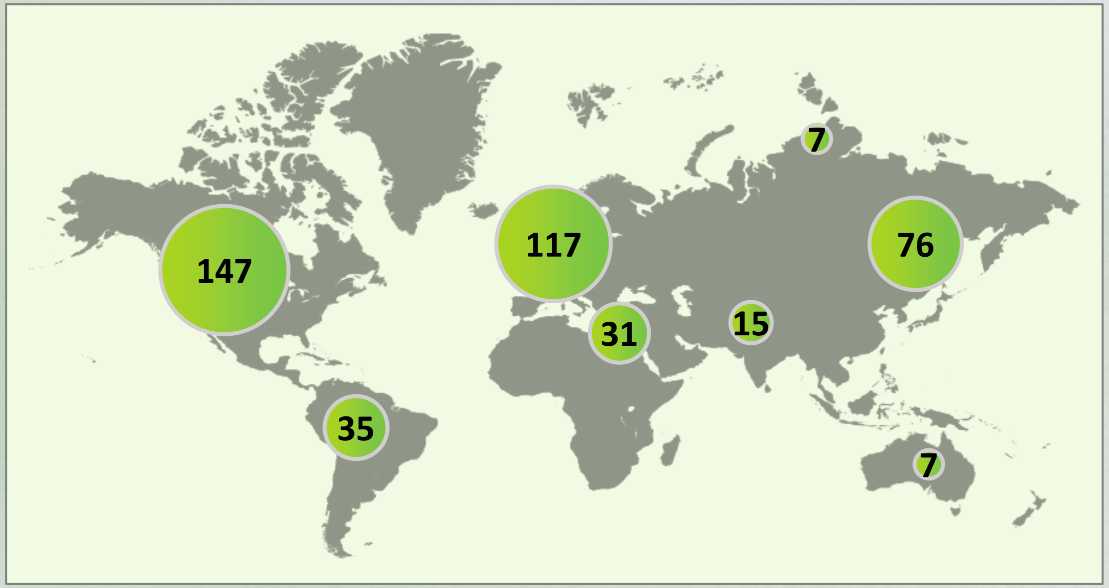
Threat vector highlight | Underground threat trends

Deloitte CTI actively monitors multiple underground forums and cybercriminal marketplaces where threat actors trade goods, data, malware and services. This slide illustrates the overarching trends for the targets by region and industry globally, and the type of services or goods being sold between January–June 2025.

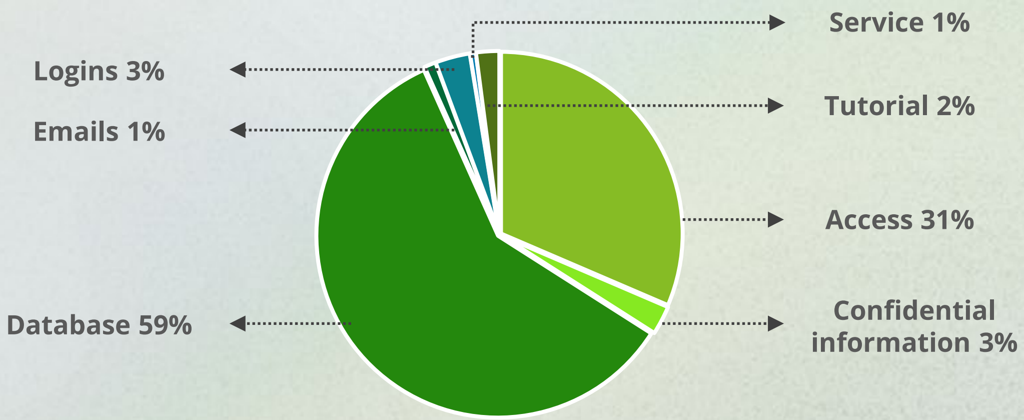
Services include Distributed Denial of Service (DDoS), fully undetectable (FUD) encryptors, cryptocurrency clippers, SMS grabbers, Endpoint Detection and Response (EDR) killers, and many more.

Access can include selling licenses for popular EDR agents' software.

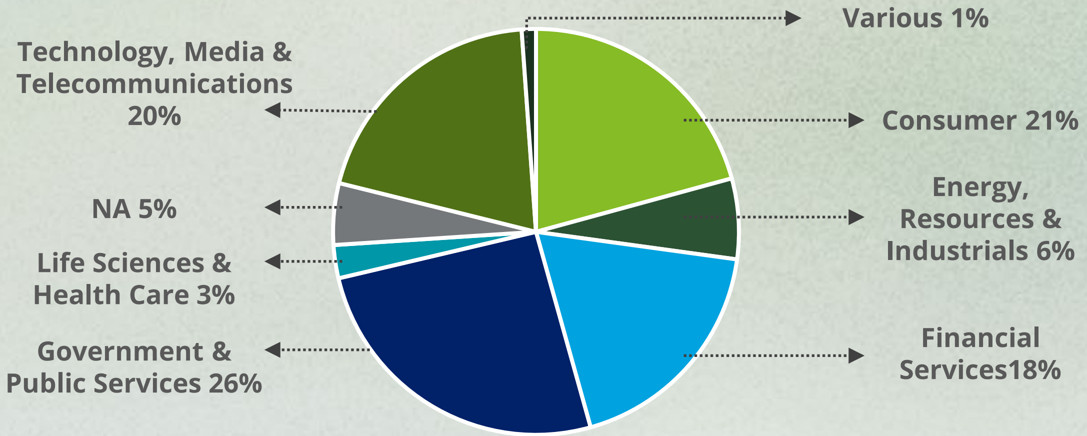
Targets by region



Distribution of items for sale



Targets by industry



Threat vector highlight | Ransomware threat trends

During the first half of 2025, ransomware trends were defined by group disruptions, affiliate shifts, and evolving extortion tactics. This slide outlines key developments in affiliate migration and operator methods.

Overview

Ransomware continues to represent a **major cyber threat in 2025, driven by a fluid ecosystem of affiliates, adaptable tooling, and financially-motivated operators**. The first half of the year has been defined by both disruption and resurgence. **High-profile outages** such as the RansomHub takedown temporarily **reduced activity but also triggered rapid affiliate migration** to more stable groups like Qilin, which experienced a significant surge in disclosed victims [4], [15].

At the same time, **ransomware operations have matured in strategy and structure.** Multi-extortion is now standard, combining encryption, data theft, reputational threats, and regulatory pressure [16], [17]. Many groups are adopting modular toolchains and polished data leak sites to attract affiliates and build credibility [18], [19]. These developments reflect a more professional, business-like approach to extortion [20], [21] .

Affiliate migration trends

- RansomHub, one of the most prolific ransomware groups in early 2025, ceased operations at the beginning of April. Its data leak site went offline without warning and remains inactive at the time of this writing, with no official explanation or confirmed law enforcement action at the time [4], [15]. This outage disrupted a key part of the ransomware ecosystem and led to a temporary reduction in publicly-disclosed victim data across multiple sectors.

- In the aftermath, Qilin emerged as the most active ransomware group globally, claiming 74 attacks in April. The close timing between RansomHub going offline and Qilin's rise suggests that many of those affiliates may have migrated to Qilin. In doing so, they likely sought operational continuity, access to stable infrastructure, and a trustworthy platform to continue their extortion campaigns without significant disruption [15].

- Although direct attribution of affiliate movement is difficult, the correlation between RansomHub's disappearance and Qilin's growth highlights the fluid structure of the RaaS model. Affiliates often align themselves with groups that offer visibility, support, and payment reliability. As a result, the outage of a single group can quickly reshape the broader threat landscape [4], [15].

- In the aftermath of RansomHub going dark, DragonForce positioned itself as a new home for displaced affiliates. By advertising a decentralized cartel model that let affiliates use their own ransomware and branding, DragonForce created a compelling alternative to the standard RaaS model. Multiple affiliates, including those behind VanHelsing and RansomBay, are believed to have made the switch [3].

Evolving ransomware playbook

- Ransomware operators in 2025 are expanding their use of multi-extortion tactics to increase leverage over victims. Along with data encryption, threat actors conduct data theft, reputational threats, and ongoing threat campaigns that cause regulatory pressure across industries. Anubis, for example, employs a three-tiered model combining traditional ransomware, data-only extortion, and access monetization strategies [16], [17].

- Technical execution has also evolved. Groups such as Qilin leverage modular toolchains built around advanced loaders like SmokeLoader and NETXLOADER, supported by reflective dynamic link library (DLL) injection and Rust-based components [18]. Trojans detected in recent intrusions include Emotet, Sirefef, and Hesperbot and often used to gain access, escalate privileges, and enable lateral movement before ransomware deployment [19].

- Structurally, ransomware groups are increasingly adopting professional service models. DragonForce, for example, enables affiliates to operate under their own distinct brands while leveraging shared infrastructure, including client panels, negotiation tools, and a Tor-based leak site [17]. Ransomware groups now mirror legitimate businesses, offering affiliate tiers, onboarding support, and profit-sharing models, complete with admin dashboards and negotiation tools to attract and retain partners [20].

- There is a noticeable split in ransomware tactics. Some threat actors maintain traditional double extortion models, encrypting data and threatening to leak it. Others now skip encryption altogether. These groups opt for a more streamlined approach, exfiltrating data and immediately using the risk of public disclosure as leverage. This simplifies operations and helps them evade some ransomware-specific defenses [16].

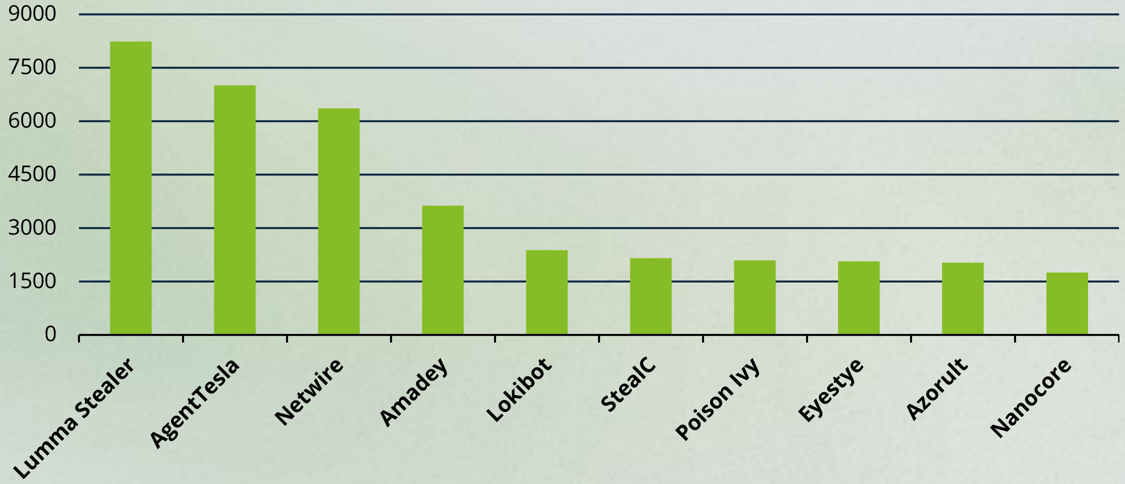
Threat vector highlight | Infostealer malware

Affiliate migration trends

In 2025, there have been two large scale coordinated takedowns of infostealer malware and its infrastructure. These takedowns have led to the disruption of LummaStealer and a number of arrests for individuals involved in Operation Secure.

- **Lumma Stealer:** In May, a coordinated global takedown involving law enforcement agencies in Europe, the US, and Japan, seized over 2,300 domains and dismantled Lumma's infrastructure. This operation identified nearly 400,000 computers that had been infected with the malware globally. Although a drop in Lumma Stealer-linked credentials stolen is expected as a result of this operation, it is expected to remain as a persistent threat due to its high popularity and its Malware-as-a-Service (MaaS) model [7]. At the time of publishing, reports have highlighted that the infrastructure is back up and running.
- **Operation Secure:** Between January and April, an Interpol-led operation known as Operation Secure led to the take down of over 20,000 malicious IPs and domains, along with the seizure of 41 servers, 100GB of data collected, and 32 arrests. The operation involved law enforcement agencies from 26 countries in Asia and the South Pacific and coordinated with private sector partners. The effort resulted in the takedown of 79 percent of identified suspicious IP addresses. Over 216,000 victims and potential victims were notified following the operation [21].

Top 10 malware strains observed by Deloitte CTI between January – June 2025



Affiliate migration trends

In 2025, many infostealers went through advancements, which in turn highlights the capabilities of its developers and emphasises that these stealers will continue to persist.

- **Lumma Stealer:** In 2025, reports of Lumma Stealer advancements and growth were observed. It was noted that the new version utilized fake CAPTCHA prompts to steal credentials and to ultimately evade detection. Lumma has been noted as quite sophisticated particularly due to the broad, evolving list of delivery vectors that it leverages, including phishing emails and malvertising [7].
- **StealC:** In March, the second iteration of StealC—an infostealer and malware downloader—was released. This version included multiple updates including a streamlined command and control (C2) protocol, expanded malware payload delivery options, and server-side brute forcing for credentials. It has been noted that StealC conducts validation steps before executing the payload, one of which filters for regional languages that indicate the threat actor's origin [8] [9].
- **Vidar Stealer**: Recent reporting on Vidar Stealer highlights that its return has been linked with an upgraded version. The new version has been observed to masquerade as a tool that is commonly trusted by IT teams. Vidar Stealer is known to target browser credentials, cookies and session token, cryptocurrency wallets, and cloud credentials [1].

Mid-year cyber threat trends 2025

Threat actors | Overview

Nation-state linked

Motivation	Political, Espionage, Financial
Likelihood	Likely, Significant long-term impact
Top Actors	APT28, Lazarus Group

- Nation state-linked hackers (APT28) targeted Western logistics and defense firms to gather intelligence on aid shipments to Eastern Europe, using spear phishing and small network exploits [22].
- Nation state-linked actors used the ClickFix technique in early 2025 phishing campaigns, tricking targets into executing malicious commands via fake system instructions. [23]

Cybercriminals

Motivation	Financial
Likelihood	Likely, Significant immediate impact
Top Actors	Akira Ransomware, Qilin, DragonForce, Sarcoma Ransomware, Scattered Spider

- RansomHub's infrastructure shutdown triggered affiliate unrest, with many members reportedly migrating to groups like Qilin or joining DragonForce's newly formed ransomware cartel [3].
- Qilin, also known as Agenda, became the most active ransomware group in April with 72 disclosed victims, leveraging a new stealthy loader called NETXLOADER to deploy payloads like SmokeLoader and Agenda ransomware, with targeted attacks on health care, technology, and financial sectors across multiple global regions [24].

Hacktivists

Motivation	Political
Likelihood	Roughly even chance, Moderate impact
Top Actors	DieNet, Dark Storm Team

- Industrial control systems (ICS) and operational technology (OT) networks experienced a significant spike in attacks in March, largely attributed to politically-aligned hacktivist activity [25].
- DieNet emerged in March 2025 as a politically- and ideologically-motivated hacktivist group targeting North America and allied critical infrastructure, including financial systems, energy grids, transportation networks, telecommunications, and other public and private-sector organizations [26].

Insider threat

Motivation	Financial, Revenge, Fear (blackmailed)
Likelihood	Malicious: Roughly even chance, Severe impactUnintentional: Likely, Significant impact
Top Actors	Not applicable

- Insider threats now cost organizations an average of USD $17.4 million per year, with containment delays significantly increasing overall impact [27],
- Ransomware groups like Sarcoma and DoNex are embedding recruitment messages in ransom notes, appealing to insiders with promises of financial rewards in exchange for internal access [28].

Threat Actors | Trending and emerging between January to June 2025

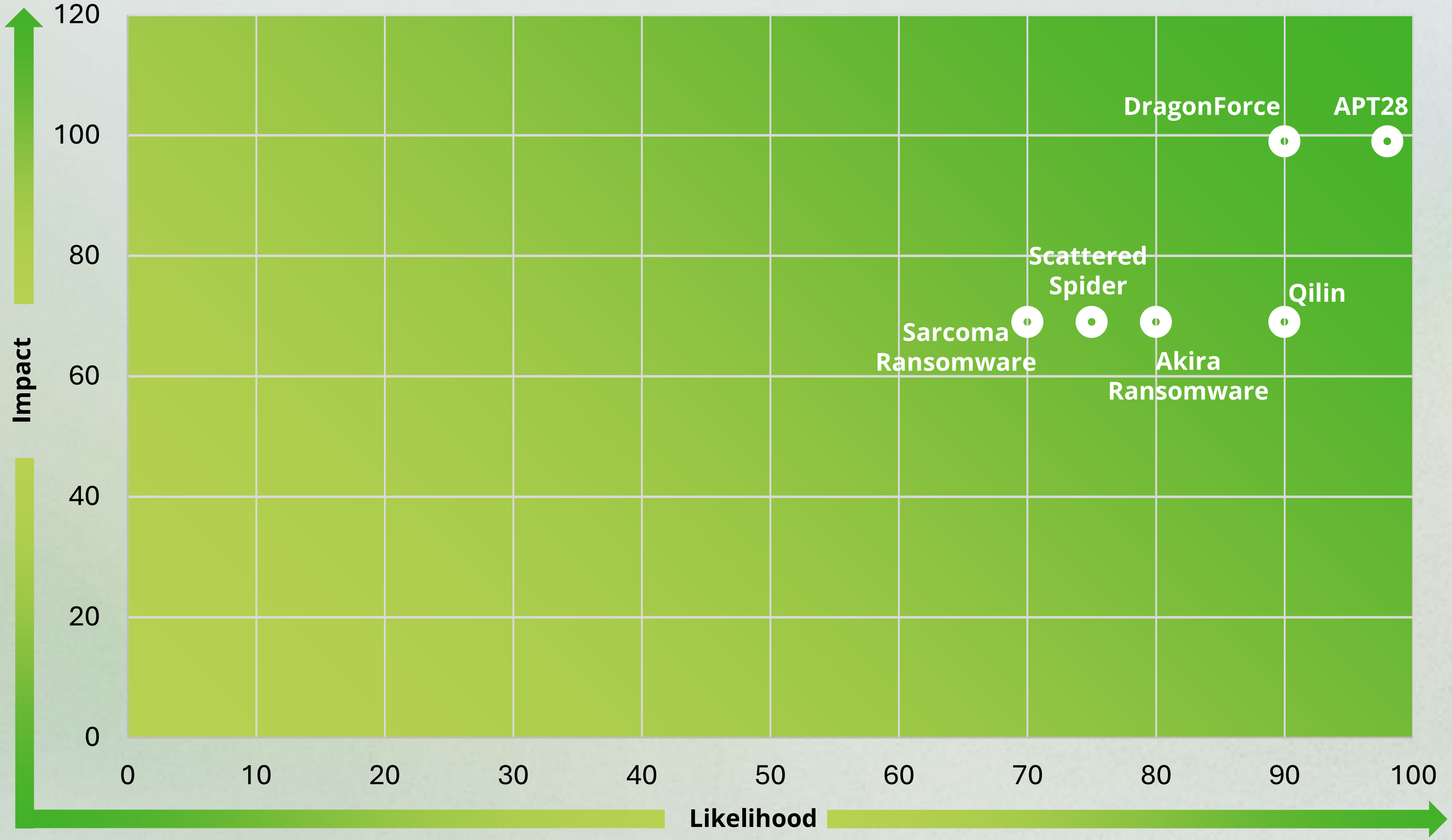


Figure 3: Top trending malware heatmap in 2023 [1]

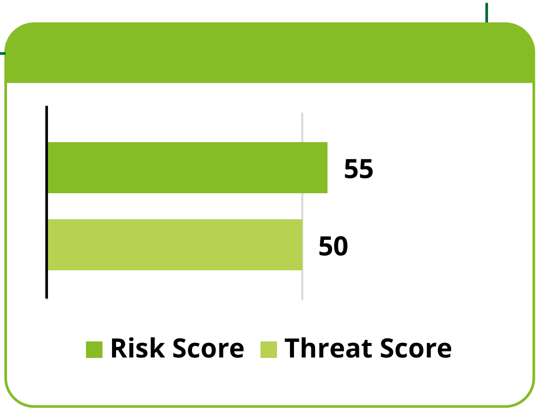
This image highlights the most trending and impactful threat actors over the last year in both frequency and spread of campaign, as well as newly emerging. Deloitte CTI analysts conducted a probability-based risk assessment to provide contextual risk quantification for the threat actors that meet these 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 is 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.

Threat actor profiles | Trending and emerging

Affiliate migration trends

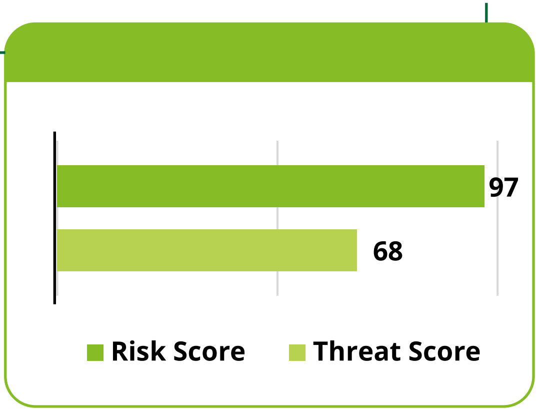
Category	Cybercriminal
Motive	Financial gain
Likelihood	Likely
Impact	Significant



- Active since March 2023, Akira Ransomware has struck over 250 organizations globally, spanning critical infrastructure, education, manufacturing and more. By early 2024, it amassed roughly $42 million in ransom payments, and in late 2024 it leaked 73 victims' data in a single month [29]
- Akira Ransomware expanded to multiple operating system targets by April 2023. In August 2023, it introduced a Rust-based variant (Megazord) [29]. The threat actor group continues to use both the Rust malware and its original C++ ransomware, exfiltrating data for double-extortion prior to encryption [30].
- Akira functions as a RaaS entity, enlisting affiliates to carry out attacks for a share of the profits. Industry analysis suggests Akira's operators may include alumni of the Conti ransomware group [30].

APT28

Category	State-sponsored group
Motive	Political gain & Espionage
Likelihood	Almost Certain
Impact	Severe

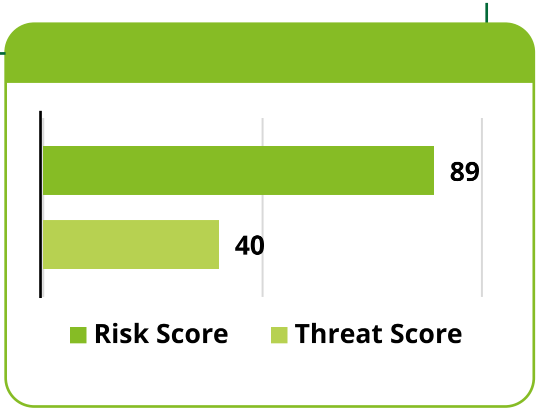


- APT28 (a.k.a. Fancy Bear) continues to conduct cyber espionage against geopolitical targets. A recent campaign shows APT28 targeting Western logistics and IT firms involved in foreign aid, as well as government and defense entities in NATO countries [2].
- In late 2023, researchers uncovered "Operation RoundPress" in which APT28 exploited webmail software via cross-site scripting (XSS) vulnerabilities to deploy a spyware (dubbed "SpyPress") and breach government and defense email systems. The group also leveraged known vulnerabilities to gain initial access to networks [2].
- APT28 still relies on tried-and-true methods like password spraying and spear-phishing to steal credentials, then modifies email permissions to maintain long-term email access to intelligence collection. They have been observed using custom implants for persistence (e.g., the "HeadLace" malware) [2].
- Western agencies have increased pressure on APT28. In 2025, 21 allied intelligence agencies jointly exposed the group's tactics and targets [2]. While under intense scrutiny, APT28 continues its espionage operations by reusing and refining its toolset in response to defensive measures.

Threat actor profiles | Trending and emerging

DragonForce

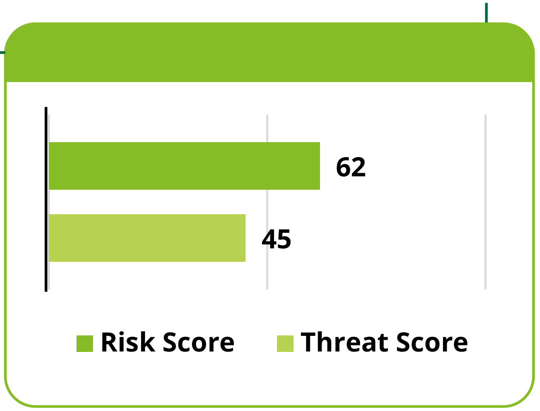
Category	Cybercriminal
Motive	Financial gain
Likelihood	Very Likely
Impact	Severe



- DragonForce emerged in 2023 from a hacktivist collective and has since pivoted from ideological attacks to profit-driven ransomware operations [31]. Once blending activism with cybercrime, it now functions as a RaaS outfit focused on financial extortion [32].
- DragonForce has launched attacks worldwide. Its victims span retail, financial, manufacturing, health care, and government sectors across North America, Europe, and Asia [32].
- The group's tactics blend common tools with aggressive extortion. DragonForce affiliates gain access via phishing, known exploits, or stolen credentials. Once inside, they deploy Cobalt Strike for lateral movement, Mimikatz for credential theft, and the SystemBC backdoor for persistence. Attacks follow a double-extortion model, encrypting files while exfiltrating data to a Tor leak site [32].
- In 2025, DragonForce openly feuded with rival RansomHub (taunting the gang's collapse), fueling speculation that DragonForce either rebranded from RansomHub or was vying for RaaS dominance [32].
- Operating as a RaaS "cartel", DragonForce equips affiliates with ransomware tools and infrastructure. It maintains a browser-based "DragonLeaks" leak portal to publish stolen data and handle negotiations. Affiliates use a web panel to customize payloads, receive technical support, and split ransoms via a tiered commission model [32].

Qilin

Category	Cybercriminal
Motive	Financial gain
Likelihood	Likely
Impact	Significant

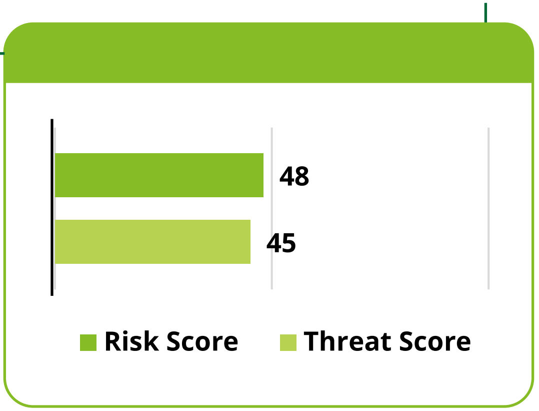


- Qilin has rapidly become one of the most active ransomware actors. After rebranding to Qilin in late 2022, it steadily ramped up operations through 2023 and then surged in 2025 – leading all groups with 72 victim postings in April 2025 and over 300 victims claimed in the year's first half. Its attacks span many industries globally, filling a void left by several rival gangs' decline [33].
- In 2025 Qilin introduced a novel extortion tactic by adding a "Call Lawyer" button to its affiliate portal. This offers affiliates on-demand legal counsel to threaten victims during negotiations – for example, having a fake lawyer join chat discussions to apply pressure [33].
- As a RaaS platform, Qilin provides affiliates with advanced tools and support. Its malware (written in Rest and Go) is cross-platform and features secure boot bypass and anti-detection measures. The affiliate panel automates tasks like network propagation, log cleanup, and ransom negotiations, and event offers DDoS and spam services plus "in-house" leak site content writers. This sophisticated ecosystem—combined with a generous profit share for affiliates—has attracted many former RansomHub partners to Qilin's program [33].

Threat actor profiles | Trending and emerging

Sarcoma Ransomware

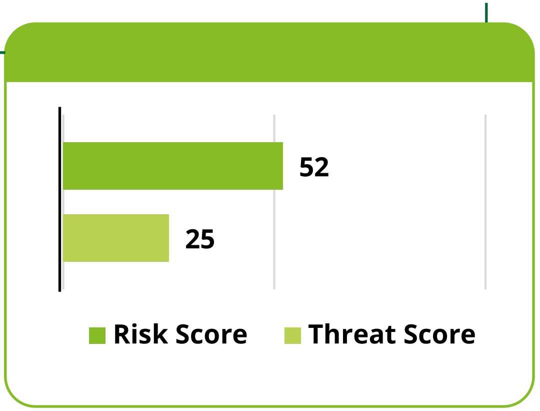
Category	Cybercriminal
Motive	Financial gain
Likelihood	Likely
Impact	Significant



- Sarcoma is a new ransomware group (first observed in October 2024) that quickly escalated its activity. By Q1 2025, Sarcoma was responsible for about two percent of industrial ransomware incidents worldwide [34].
- Sarcoma's double-extortion attacks have hit high-value organizations across various sectors, with a focus on manufacturing and supply chain companies [34]. Sarcoma has targeted global tech and logistics firms, causing significant disruption and data exposure.
- The group employs common by effective techniques for initial access: spear-phishing emails and exploitation of known vulnerabilities in remote access systems. In some cases, Sarcoma has compromised IT service providers to pivot into client networks. Once inside a victim network, Sarcoma uses tools like remote access systems for lateral movement and exfiltrates large data archives before executing its file encryption payload [34].

Scattered Spider

Category	Cybercriminal
Motive	Financial gain
Likelihood	Likely
Impact	Significant



- In June 2025, Scattered Spider targeted major insurers. The group employed social engineering tactics to infiltrate networks, compromising sensitive data such as Social Security numbers and health information [35].
- Despite arrests of key members in 2024, Scattered Spider continues to adapt. In 2025, the group deployed the DragonForce ransomware variant and updated their phishing kits to enhance their social engineering campaigns [36][37].
- Scattered Spider remains a significant cybersecurity threat, leveraging advanced social engineering and technical skills to target various industries.

Sources

1. Deloitte internal sources.
2. CISA, “Russian GRU Cyber Actors Targeting Western Logistics Entities and Tech Companies”, CISA, May 21, 2025. [Online], Available: https://www.cisa.gov/news-events/alerts/2025/05/21/russian-gru-cyber-actors-targeting-western-logistics-entities-and-tech-companies [Accessed: June 26, 2025].
3. Lakshmanan, R., “RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control”, The Hacker News, April 30, 2025. [Online]. Available: https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html. [Accessed: June 05, 2025].
4. Cyble, “Qilin Tops April 2025 Ransomware Report,” Cyble, 2025. [Online]. Available: https://cyble.com/blog/qilin-tops-april-2025-ransomware-report/. [Accessed: June 18, 2025].
5. Vijayan, J., “Prolific RansomHub Operation Goes Dark”, Dark Reading, May 01, 2025. [Online]. Available: https://www.darkreading.com/cyber-risk/prolific-ransomhub-operation-goes-dark. [Accessed: June 05, 2025].
6. Simonovich, V., “Cato CTRL Threat Research: WormGPT Variants Powered by Grok and Mixtral”, Cato Networks, June 17, 2025. [Online]. Available: https://www.catonetworks.com/blog/cato-ctrl-wormgpt-variants-powered-by-grok-and-mixtral/. [Accessed: June 25, 2025].
7. Khader, MA., “Unmasking the Evolving Threat: A Deep Dive into the Latest Version of Lumma InfoStealer with Code Flow Obfuscation”, Trellix, April 21, 2025. [Online]. Available: https://www.trellix.com/blogs/research/a-deep-dive-into-the-latest-version-of-lumma-infostealer/. [Accessed: July 18, 2025].
8. Toulas, B., “StealC malware enhanced with stealth upgrades and data theft tools”, Bleeping Computer, May 04, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/stealc-malware-enhanced-with-stealth-upgrades-and-data-theft-tools/. [Accessed: June 06, 2025].
9. Staff, “I StealC You: Tracking the Rapid Changes To StealC”, Zscaler, May 01, 2025. [Online]. Available: https://www.zscaler.com/blogs/security-research/i-stealc-you-tracking-rapid-changes-stealc. [Accessed: June 06, 2025].
10. Staff, “Ransomware Trends & Data Insights: April 2025”, Areteir, April 07, 2025. [Online]. Available: https://areteir.com/article/april-2025-ransomware-trends-threat-activity. [Accessed: June 05 2025].
11. Rubin, S., “Unit 42 Develops Agentic AI Attack Framework”, Palo Alto Networks, May 14, 2025. [Online]. Available: https://www.paloaltonetworks.com/blog/2025/05/unit-42-develops-agentic-ai-attack-framework/. [Accessed: June 25, 2025].
12. Bradley, T., “What Agentic AI Could Mean For Security Operations”, Forbes, April 17, 2025. [Online]. Available: https://www.forbes.com/sites/tonybradley/2025/04/17/what-agentic-ai-could-mean-for-security-operations/. [Accessed: June 25, 2025].
13. Lorber, N., “New Malware Variant Identified: ResolverRAT Enters the Maze”, Morphisec, April 14, 2025. [Online]. Available: https://www.morphisec.com/blog/new-malware-variant-identified-resolverrat-enters-the-maze. [June 06, 2025].
14. Wei Yeong, L., “Uncovering .NET Malware Obfuscated by Encryption and Virtualization”, Unit 42, March 03, 2025. [Online]. Available: https://unit42.paloaltonetworks.com/malware-obfuscation-techniques. [June 06, 2025].
15. Culafi, A., “Prolific RansomHub Operation Goes Dark,” Dark Reading, April 8, 2025. [Online]. Available: https://www.darkreading.com/cyber-risk/prolific-ransomhub-operation-goes-dark. [Accessed: June 18, 2025].
16. Northern Technologies Group, “The Evolving Landscape of Ransomware: Trends and Emerging Threats in 2025,” NTG, 2025. [Online]. Available: https://ntgit.com/the-evolving-landscape-of-ransomware-trends-and-emerging-threats-in-2025/. [Accessed: June 18, 2025].
17. Mandvi, “DragonForce and Anubis Ransomware Operators Introduce Updated Affiliate Models,” CyberPress, 2025. [Online]. Available: https://cyberpress.org/dragonforce-and-anubis-ransomware-operators/. [Accessed: June 18, 2025].
18. Cyfirma, “Tracking Ransomware: May 2025,” Cyfirma, May 2025. [Online]. Available: https://www.cyfirma.com/research/tracking-ransomware-may-2025/. [Accessed: June 18, 2025].
19. Halcyon, “Halcyon Threat Insights #012: January 2025 Ransomware Report,” Halcyon, January 2025. [Online]. Available: https://www.halcyon.ai/blog/halcyon-threat-insights-012-january-2025-ransomware-report. [Accessed: June 18, 2025].
20. Culafi, A., “Ransomware Gangs Innovate With New Affiliate Models,” Dark Reading, April 29, 2025. [Online]. Available: https://www.darkreading.com/data-privacy/ransomware-gangs-innovate-new-affiliate-models. [Accessed: June 18, 2025]. “
21. Staff, “20,000 malicious Ips and domains taken down in INTERPOL infostealer crackdown”, INTERPOL, June 11, 2025. [Online]. Available: https://www.interpol.int/News-and-Events/News/2025/20-000-malicious-IPs-and-domains-taken-down-in-INTERPOL-infostealer-crackdown. [Accessed: June 17, 2025].
22. Klepper, D., "Russian hackers target Western firms shipping aid to Ukraine, US intelligence says," Associated Press, May 23, 2025. [Online]. Available: https://apnews.com/article/6308ca3e11c8299470df573e4f422878. [Accessed: May 29, 2025].

Sourcing Statement

23. Naumaan, S., Kelly, M., Lesnewich, G., Miller, J., and The Proofpoint Threat Research Team, “Around the World in 90 Days: State-Sponsored Actors Try ClickFix,” Proofpoint Threat Insight Blog, April 17, 2025. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix. [Accessed: May 29, 2025].
24. Lakshmanan, R., “Qilin Ransomware Ranked Highest in April 2025 with 72 Data Leak Disclosures,” The Hacker News, May 8, 2025. [Online]. Available: https://thehackernews.com/2025/05/qilin-leads-april-2025-ransomware-spike.html. [Accessed: June 12, 2025].
25. Ribeiro, A., “Rise in hacktivist threats to critical sector, as pro-Russian groups cause 50% rise in ICS/OT attacks in March,” Industrial Cyber, April 22, 2025. [Online]. Available: https://industrialcyber.co/reports/rise-in-hacktivist-threats-to-critical-sector-as-pro-russian-groups-cause-50-rise-in-ics-ot-attacks-in-march/. [Accessed: May 29, 2025].
26. Radware Staff, "DieNet Activity Escalates Against US Organizations," Radware Threat Alerts, March 18, 2025. [Online]. Available: https://www.radware.com/security/threat-advisories-and-attack-reports/dienet-activity-escalates-against-us-organizations/. [Accessed: May 29, 2025].
27. Roessler, K., “2025 Ponemon Cost of Insider Risks Report: What’s Working, What’s Not, and What Now?,” DTEX Systems Blog, February 26, 2025. [Online]. Available: https://www.dtexsystems.com/blog/2025-cost-insider-risks-takeaways/. [Accessed: May 29, 2025].
28. Beek, K., “Cybercriminals Court Traitorous Insiders via Ransom Notes,” Dark Reading, February 5, 2025. [Online]. Available: https://www.darkreading.com/threat-intelligence/cybercriminals-traitorous-insiders-ransom-notes. [Accessed: June 12, 2025].
29. CISA, “#StopRansomware: Akira Ransomware”, CISA, April 18, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a [Accessed: June 26, 2025].
30. Traynor, O., “The 2025 Akira Ransomware Playbook”, CyberlAngel, February 3, 2025. [Online], Available: https://cybelangel.com/the-akira-ransomware-playbook-everything-you-need-to-know/ [Accessed: June 26, 2025].
31. Traynor, O., “Who is the DragonForce Ransomware Gang?”, CybelAngel, June 18, 2025. [Online], Available: https://cybelangel.com/who-is-the-dragonforce-ransomware-gang/ [Accessed: June 25, 2025].
32. Darkatlas Squad, “DragonForce Ransomware: From Hacktivism to Global Cyber Extortion”, Darkatlas, June 29, 2025. [Online], Available: https://darkatlas.io/blog/dragonforce-ransomware-from-hacktivism-to-global-cyber-extortion [Accessed: July 02, 2025].
33. Lakshmanan, R., “Qilin Ransomware Adds “Call Lawyer” Feature to Pressure Victims for Larger Ransoms”, The Hacker News, June 20, 2025. [Online], Available: https://thehackernews.com/2025/06/qilin-ransomware-adds-call-lawyer.html [Accessed: June 27, 2025].
34. Alamri, A., “Dragos Industrial Ransomware Analysis: Q1 2025”, Dragos, May 21, 2025. [Online], Available: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2025/ [Accessed June 27, 2025].
35. Loten, A., Rundle, J., “Insurers ‘Under Siege’ by Notorious Hacking Group”, The Wall Street Journal, June 24, 2025. [Online], Available: https://www.wsj.com/articles/insurers-under-siege-by-notorious-hacking-group-7cb68a8e [Accessed: June 30, 2025].
36. Taylor, E., “Comprehensive CTI Report: Scattered Spider Threat Actor Group”, Barricade cyber solutions, May 7, 2025. [Online], Available: https://barricadecyber.com/cti-report-scattered-spider-threat-actor-group/ [Accessed: June 30, 2025].
37. Staff, “MOXFIVE Threat Actor Spotlight – Scattered Spider”, MoxFive, June 4, 2025. [Online], Available: https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-scattered-spider [Accessed: June 30, 2025].

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 (e.g., 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 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

Deloitte.