HALL OF HACKS

Q1- 2025

Prepared by

CYBERMATERIAL

Powered by

911CYBER

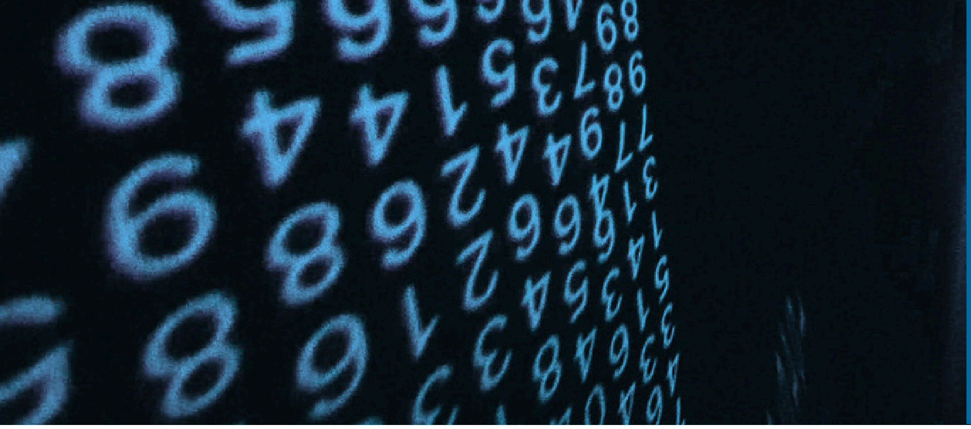


Table of Contents

Introduction

Welcome to Hall of Hacks – Q1 2025. In this edition, we present a data-driven examination of cybersecurity incidents, threats, and industry developments during the first quarter of 2025.

Figure 1. Abstract cybersecurity illustration representing the Hall of Hacks theme.

This report examines a broad spectrum of cybersecurity activity, including analyzed incidents, malicious campaigns, diverse malware families, active ransomware groups, and known threat actors. It also provides insights into newly disclosed vulnerabilities, legal actions, regulatory developments, and market trends.

Building on previous editions, our analysis incorporates data from global cybersecurity intelligence providers, public disclosures, and internal case studies. We use a consistent classification approach to categorize threat actors, attack methods, and impacted assets. Our goal is to provide security leaders, policymakers, and operational teams with clear insight into who is attacking, how they operate, and which defenses are most effective.

Executive Summary

The first quarter of 2025 paints a complex picture of cybersecurity, marked by progress, persistent threats, and devastating breaches.

The Good

- Investment & M&A Momentum: $4.4B in new cybersecurity funding and $32B in mergers and acquisitions demonstrate continued confidence in security solutions, particularly in Managed Security Services (MSS) and Threat Detection & Response.
- Regulatory & Legal Progress: 133 new cyber policies and 142 criminal judicial actions, including high-profile extraditions and the $45M MGM Resorts settlement, reinforced global accountability.
- Cross-Border Cooperation: Joint law enforcement operations disrupted ransomware groups like LockBit and 8Base, marking tangible wins for defenders.

The Bad

- Threat Surge: 545 incidents and 29 malicious campaigns were tracked, driven by 41 ransomware groups, 118 malware families, and 98 active threat actors.
- Vulnerability Explosion: 3,725 CVEs emerged in Q1, with WordPress (517), Microsoft (292), and Apple (266) leading as the most exposed vendors.
- State-Sponsored and Criminal Activity: Russia, China, Iran, and North Korea continued to dominate global APT and hybrid operations, often targeting government, defense, and financial sectors.

The Ugly

- Historic Data Breaches: Over 3.2 billion records were compromised this quarter, including 2.8B from Twitter/X alone.
- Financial Devastation: Bybit's $1.5B cryptocurrency theft marked one of the largest digital heists in history.
- Critical Sector Impact: Government, healthcare, and education absorbed the majority of attacks, highlighting ongoing systemic vulnerabilities.

Overall, Q1 2025 underscores that cyber risk is both pervasive and evolving. While investments and policy progress reflect resilience and adaptation, attackers continue to exploit vulnerabilities at scale, making intelligence-driven defense and rapid response essential for survival.

Inductees

Top Investment

SailPoint

cyera

$1.4B

Top M&A

WIZ

by Google

$32B

Top Regulation

Memorandum of Understanding (MoU) on Cybercrime Investigations

Top Judicial Action

Evan Frederick Light

$37M Crypto Theft

Sentenced

Top Threat Actor

FOG

Most Active

Top Threat

Lumma

Most Active

Top Vulnerability

CVE-2024-50603

Highest CVSS score

Most Vulnerable Vendor

WordPress

Most CVEs

Top Victim

BYBit

$1.5B Theft

Most Affected Industry

Government

Most Incidents

Most Affected Country

USA

Most Targeted

Top Legal Action

MGM Resorts International

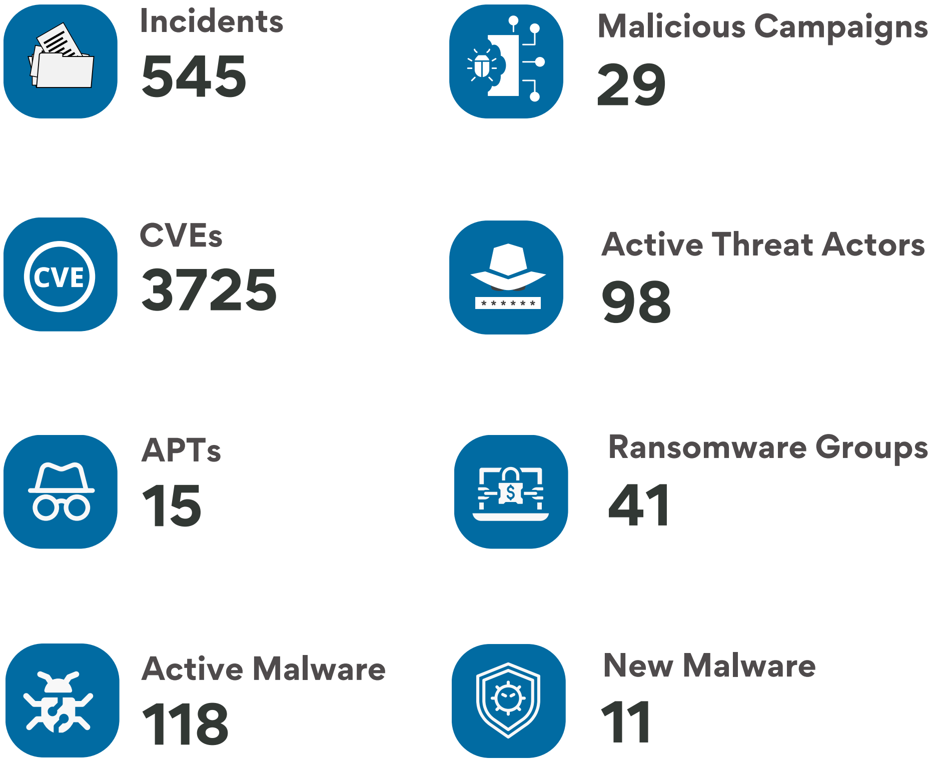
$45M - Settlement

Figure 2. List of Inductees in the Q1 2025 Hall of Hacks

Findings

Highlights

The first quarter of 2025 presented a dynamic and challenging cybersecurity environment. Our analysis reveals a significant volume of malicious activity, including a total of 545 incidents and 29 malicious campaigns detected. Threat actors remained highly active and innovative, with a record number of 41 ransomware groups and 118 active malware entries operating in the wild. This quarter also saw the emergence of 11 new malware variants, adding to the active malware strains currently in circulation. The data further highlights the persistent threat from state-sponsored groups, with 15 APTs (Advanced Persistent Threats) identified. Finally, the quarter underscored the ongoing importance of vulnerability management, with 3725 CVEs (Common Vulnerabilities and Exposures) being a key point of focus for defenders and attackers alike.



Incidents
545

Malicious Campaigns
29

CVEs
3725

Active Threat Actors
98

APTs
15

Ransomware Groups
41

Active Malware
118

New Malware
11

Figure 3. Key Findings Overview of Hall of Hacks Q1 2025

Financing

Funding

The first quarter of 2025 showed significant activity in investments, with several large-scale funding rounds. Five standout investments led the period: SailPoint raised $1.4B in a IPO round (Identity and Access Management (IAM), ReliaQuest raised $500M in a Private Equity round (Threat Detection & Response), NinjaOne raised $500M in a Series C Extension round (Endpoint Security) ID.me raised $275M in a Debt Financing round (Identity & Access Management (IAM)) Island raised $250M in a Series E round (Endpoint Security) These highlights indicate sustained investor confidence in companies tackling critical challenges across various segments.

Total Investments

142

Figure 4. Total amount of investments — Q1 2025

The first quarter of 2025 showcased significant momentum in the investment sector, marked by substantial funding rounds across various sectors. Leading this period were several impressive investments.

Top Invesments

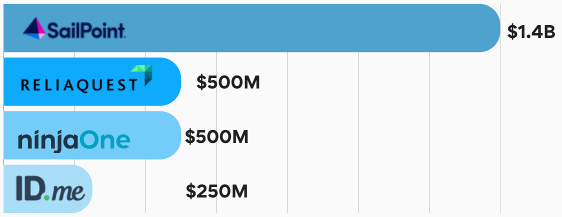


Figure 5. Top 5 Cybersecurity Investment Rounds — Q1 2025

Highlights

Beyond these large-scale deals, the quarter also saw diverse activity across numerous segments. While specific early-stage investment numbers were not detailed in the top highlights, the overall breadth of segments receiving funding, including AI, Cybersecurity, Digital Health, Fintech, and Renewable Energy, suggests a healthy and diversified investment environment. This widespread interest indicates that investors are not only backing mature entities but are also keen on supporting innovation across a broad spectrum of emerging and critical areas, reinforcing the dynamic growth observed in the early months of 2025.

Investment Segments

39	Threat Detection & Response
25	Application & Software Security
18	Identity & Access Management (IAM)
14	Governance, Risk & Compliance (GRC)
13	Data Protection
8	Network & Infrastructure Security
7	Managed Security Services (MSS)
7	Security Awareness & Training
7	Endpoint Security
4	Cloud Security

Figure 6. Total Cybersecurity Investments by Segment — Q1 2025

Financing

Mergers & Acquisitions

Managed Security Services (MSS) Leads M&A Activity: The most significant volume of M&A deals in Q1-25 was concentrated in Managed Security Services, underscoring a strong market demand for outsourced security solutions.

Strong Focus on Proactive Defense and Threat Detection: 'Threat Detection & Response' emerged as the second most active segment, indicating a strategic emphasis on solutions that proactively identify and mitigate cyber threats.

Dominance of the U.S. Market: The United States overwhelmingly leads in both the number of acquiring and acquired companies, highlighting its central role in the global cybersecurity M&A ecosystem.

Sector	#Deals
Managed Security Services (MSS)	27
Threat Detection & Response	21
Network & Infrastructure Security	13
Governance, Risk & Compliance (GRC)	10
Data Protection / Security	9
Identity and Access Management (IAM)	8
Application & Software Security	7
Cloud Security	4
Endpoint Security	4
Security Awareness & Training	2

Figure 7. Leading Security Segments in M&A Activity

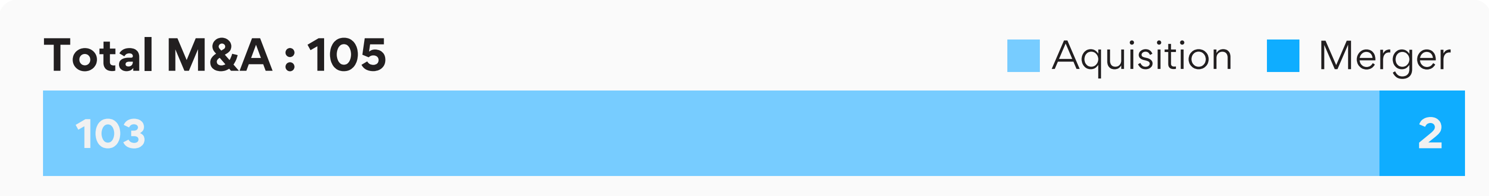
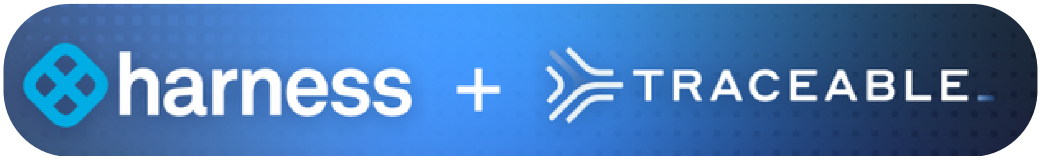


Figure 8. Total M&A Deals in Cybersecurity — Q1 2025

Top Merger



Top Aquisition

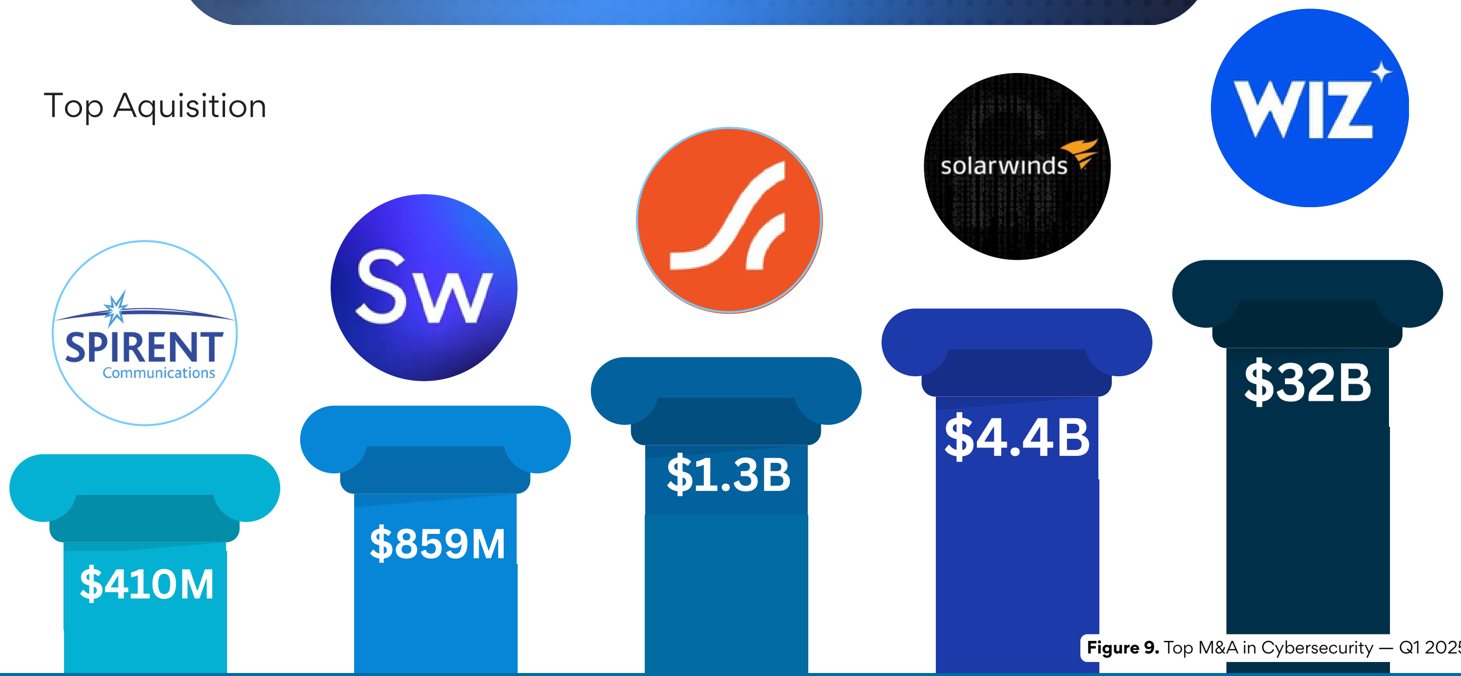


Figure 9. Top M&A in Cybersecurity — Q1 2025

Financing

Key Insights, forecast and recommendations

Insights:

- **Capability-Driven Market:** The M&A sector is overwhelmingly driven by the strategic imperative to acquire and integrate specific cybersecurity capabilities (e.g., threat detection, managed services, platform enhancements) rather than simply consolidating market share. Companies are buying solutions and expertise to fill gaps and fortify their offerings.

- **Essential Role of Outsourced Security:** The sustained leadership of Managed Security Services (MSS) in M&A activity highlights the growing reliance of enterprises on outsourced security functions. This indicates a continuing trend towards specialized providers handling complex security operations.

Forecast:

- **Sustained M&A Momentum**: Given the high volume of "Announced" deals in Q1-25 and the strategic necessity for security solutions, the cybersecurity M&A market is likely to remain highly active throughout 2025.

- **Continued Dominance of MSS and Threat Detection:** Deals in Managed Security Services (MSS) and Threat Detection & Response are expected to continue leading M&A activity. Enterprises will likely increase their demand for outsourced security and advanced threat mitigation capabilities, driving further consolidation and acquisitions in these segments.

- **U.S. to Remain the Epicenter:** The United States is projected to maintain its position as the dominant market for both buyers and sellers in cybersecurity M&A, though international activity, particularly from the UK, Israel, and France (sellers), and Canada and Sweden (buyers), will likely continue to grow.

Recommendations for Stakeholders:

- Strategic Investment in MSS and Threat Detection: Companies looking to grow through M&A should prioritize opportunities within the MSS and Threat Detection & Response segments, as these are the most active and in-demand areas.

- Monitor Emerging Markets: Keep an eye on countries like Israel and France as potential sources of innovative cybersecurity solutions, and Canada and Sweden as growing markets for acquisitions.

- For Global Cybersecurity Players: Broaden your acquisition scouting to include high-innovation hubs like Israel and France for cutting-edge seller technologies, while continuing to prioritize the dominant U.S. market for both acquisition and expansion opportunities. Consider Canada and Sweden as emerging buyer markets for strategic partnerships.

Cyber Policies

133

Q1 New Policies

The global cyber policy climate in Q1 2025 appears to be characterized by a robust legislative push towards comprehensive data privacy and cybersecurity measures. While the specifics vary by country, there's a clear global recognition of the need to address cyber threats, protect digital rights, and regulate emerging technologies.

Focusing on establishing consumer data rights, securing digital infrastructure and AI policies.

36	**Bills**
32	**Regulations**
28	**Guidelines**
20	**Laws**
8	**Amendments**
6	**Executive Order**
2	**Agreements**

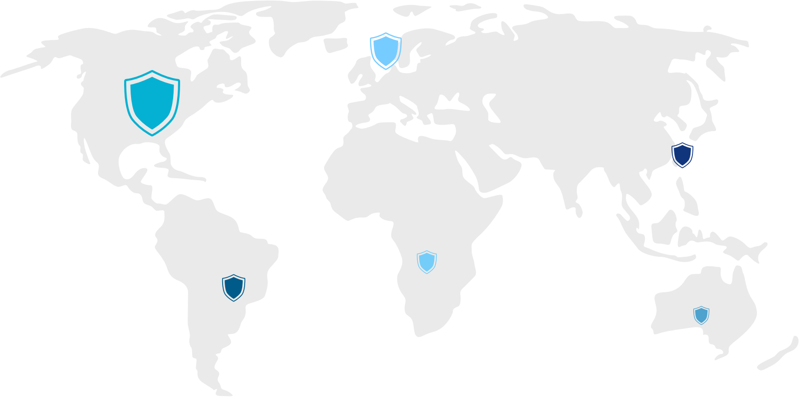


Figure 10. Map of Policies Across the World — Q1 2025

Highlights

Geographically, the reach of these cyber policies is extensive, spanning 34 countries. This widespread distribution underscores the global recognition of cybersecurity as a critical national and international concern. While the data includes major economies like the United States, China, European Union, and the United Kingdom, it also features a significant presence from diverse regions such as Southeast Asia (Singapore, Vietnam, Malaysia, ASEAN), Africa (Rwanda, Botswana, Uganda, Zimbabwe), and Latin America (Chile, Mexico, Peru).

Cyber Policies

US State-Level Comprehensive Privacy Laws

A significant number of "Law" entries, particularly from the United States, are state-level comprehensive data privacy acts such as the Delaware Personal Data Privacy Act (DPDPA), Iowa Consumer Data Protection Act (ICDPA), Nebraska Data Privacy Act (NDPA), and New Hampshire Privacy Act (NHPA). These laws are crucial because they establish fundamental consumer rights regarding personal data, including access, correction, deletion, and opt-out options for data sales or targeted advertising. Their proliferation across various U.S. states signifies a growing emphasis on individual data sovereignty and a fragmented, yet increasingly robust, privacy sector in the absence of a single federal comprehensive privacy law.

EU's Digital Operational Resilience Act (DORA) and Cyber Solidarity Act

The Digital Operational Resilience Act (DORA) provides a comprehensive framework for financial institutions to manage and recover from ICT disruptions and cyber threats, given the sector's criticality. It sets uniform standards for ICT risk management, incident reporting, and third-party risk management. Complementarily, the Cyber Solidarity Act aims to bolster the EU's collective ability to detect, prepare for, and respond to cyber threats, promoting a unified cyber defense across member states, notably through initiatives like the European Cybersecurity Alert System.

China's Network Data Security Management Regulations and AI-related Measures

These regulations integrate and clarify cybersecurity obligations for data processing, imposing new requirements on entities operating in China. Furthermore, measures such as the Administrative Measures for Personal Information Protection Compliance Audit and Facial Recognition Measures underscore China's stringent approach to enforcing personal information protection and controlling emerging technologies, impacting data governance and privacy across its digital infrastructure.

Agreement

Memorandum of Understanding (MoU) on Cybercrime Investigations

Figure 11. Agreement between India and United States of America— Q1 2025

Criminal Judicial Actions

International law enforcement bodies, including the U.S. Department of Justice, UK Police, and African authorities, coordinated extensive global operations targeting diverse cybercriminal activities such as ransomware, large-scale fraud rings, and child sexual abuse material (CSAM) networks. These efforts resulted in significant arrests and disruptions, including the extradition of an alleged LockBit developer and actions against the 8Base ransomware group, notably for their use of the Phobos variant. Additionally, investigations led to indictments against state-backed hackers like APT27 and widespread crackdowns on various online scams and illicit platforms.

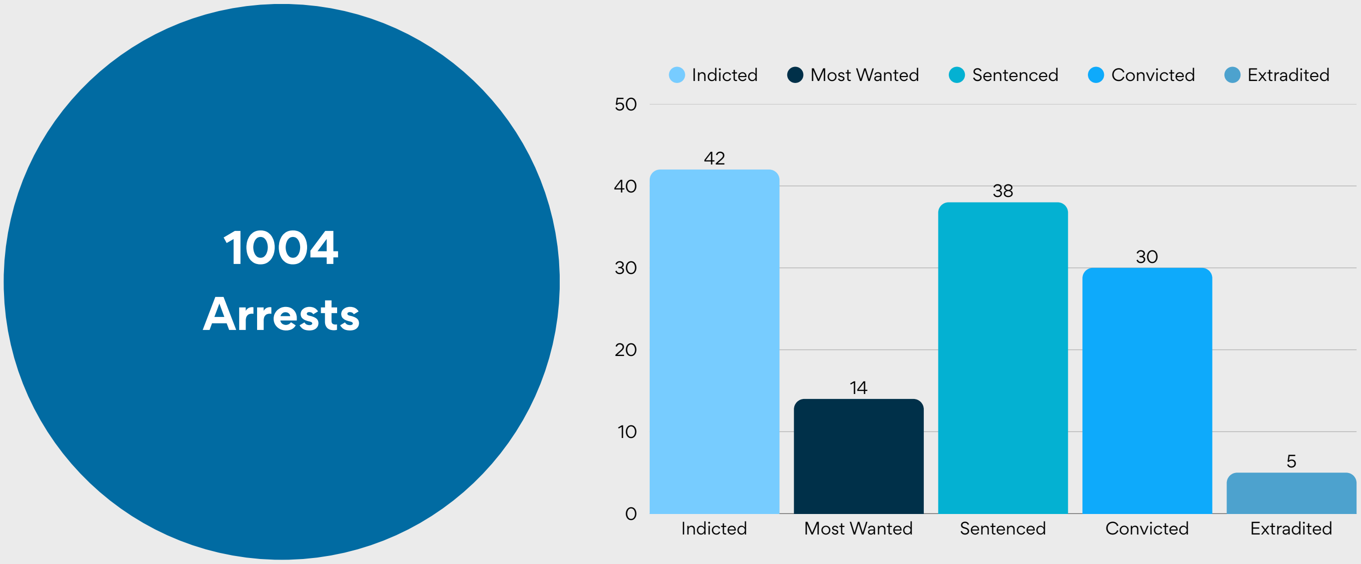


Figure 12. Global Arrests and Judicial Actions Related to Cybercrime — Q1 2025

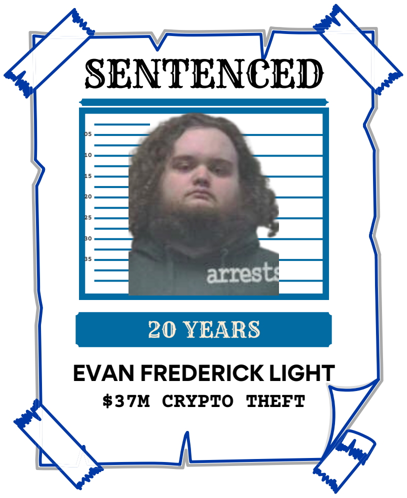


Figure 13. Top Criminal Judicial Action — Q1 2025

International law enforcement arrested and extradited key figures from prominent cybercrime entities, including **Rostislav Panev**, an alleged **LockBit** developer, whose apprehension marks a significant disruption to that ransomware operation. Separately, 2 Chinese-nationals (**APT27**), were indicted for years of espionage and financial theft targeting various U.S. sectors. Further actions included arrests and server seizures linked to the **8Base ransomware** group, notably their use of the **Phobos ransomware** variant, demonstrating broad coordinated efforts against diverse cybercriminal syndicates.

Criminal Judicial Actions

Key Insights

142 judicial actions

- January: 27 actions
- February: 55 actions
- March: 60 actions

Financial Impact - Penalties

$2B

Approximately

Figure 14. Estimate cost of financial impact from penalties (perpetrators) — Q1 2025

Indicted

2 Chinese Nationals:
State-Sponsored Hacking, Computer Intrusion, Data Theft, Espionage (**APT27**)

Sanctioned

10 Chinese Nationals:
State-Sponsored Hacking, Computer Intrusion, Data Theft, Espionage (**AQUATIC PANDA**)

Convicted

Cameron John Wagenius (Alias: Kiberphant0m)
Part of Snowflake hacking/extortion group to AT&T

Sentenced

Austin Michael Taylor
(Founder of **CluCoin**)
Wire fraud related to Miami-based cryptocurrency token CluCoin.

⚠ 5 Extraditions

Law enforcement actions have extradited a range of cybercriminals to the US, from individuals like Douver T. Braga and Aleksei Andriunin involved in cryptocurrency fraud and market manipulation, to Rostislav Panev, an alleged LockBit ransomware developer, and others engaged in phishing, malware, and tech support fraud schemes across multiple countries including Brazil, Russia, Nigeria, and the UAE.

Threat Actors

The Q1 2025 dataset captures 282 documented threat actor activities worldwide, spanning a diverse range of cyber operations including advanced persistent threat (APT) campaigns, state-sponsored espionage, cybercriminal schemes, ransomware assaults, and hacktivist initiatives. Many actors appear repeatedly across different incidents, emphasizing their ongoing roles in the cyber domain. The data highlights the significant influence of Russia, China, Iran, and North Korea in state-backed and APT operations, while Eastern Europe and groups of uncertain origin contribute notably to ransomware and cybercriminal activities.

Prominent and long-standing groups like **FOG**, **Akira**, **RansomHub**, **LockBit 3.0**, and **8Base** continue to dominate the scene, alongside numerous emerging and lesser-known actors that add complexity to the global threat landscape. This overview of Q1 2025 underscores both the geographic breadth and the persistent, multifaceted challenges facing cybersecurity today.

Q1 -25: Active Threat Actors

● Cybercriminals

NoName057(16), Natohub, BlackLock, Hunters International, Yellow drift, Belsen Group, IntelBroker, 0mid16B, Kairos, Funksec, EC2 Grouper, Codefinger, TRIPLESTRENGTH, Zodiac Killer, b0nd, Valerie, Emirking, Tooda, Stargazer Goblin, CryptoBytes, RedCurl, DragonRank, puppygirl hacker polycule, Dark Storm Team, rose87168, CoreInjection, GHNA, Lotus Blossom, Cyber Av3ngers, FamousSparrow, Gamaredon, Crazy Evil, FIN7

● State Sponsored Actors

UNC5337, Silk Typhoon, UAC-0057, Silk Typhoon, MuddyWater

● APTs

APT10, APT73, APT41, APT38, APT28, APT27, Star Blizzard, APT-C-35, APT42, APT45, APT44, Stately Taurus, APT43, Silver Fox, APT37, ScarCruft, SideWinder, RedCurl, APT-C-36

● Hacktivists

Cyber Alliance Group, Handala, ExploitWhispers, Anonymous Hacker collective

● Ransomware Groups

LockBit 3.0, Qilin, RansomHub, Hunters International, Everest, FOG, Hellcat, ThreeAM, Abyss, 8Base, CLOP, Akira, Lynx Group, DragonForce, Medusa, Babuk, Money Message, Sarcoma, Funksec, 0mid16B, Monti, Termite, Nitrogen, Belsen Group, STAC5143, PureCrypter, BianLian, INC, Crazy Hunter, Play, Lynx, Rhysida, Brain cipher, BlackLock, InterLock, RansomHouse, Arkana Security, Weyhro, Safepay, EncryptHub, Azael

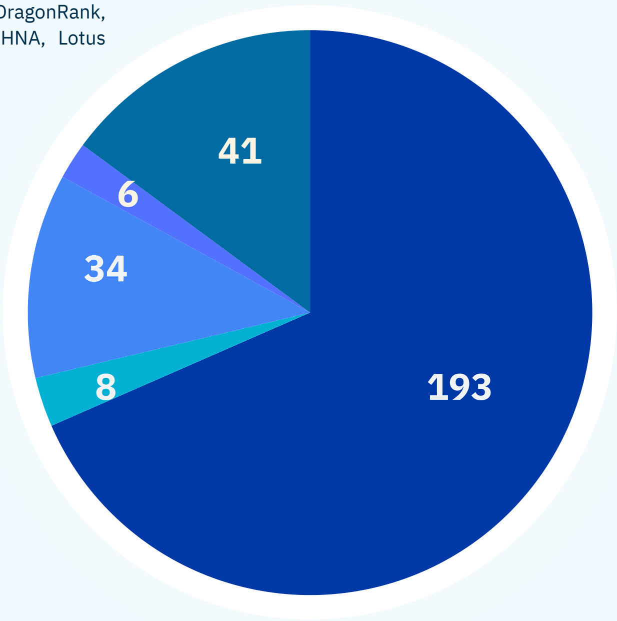


Figure 15. Number of entries per type of threat actor — Q1 2025

Threat Actors

98 Threat Actors Involved in **282** activities

RUSSIA (90)

LockBit 3.0
Qilin
NoName057(16)
CLOP
Akira
Medusa
Sarcoma
Kairos
Funksec
Termite
RedCurl
EC2 Grouper
APT28
Star Blizzard
UAC-0057
STAC5143
BianLian
APT44
CryptoBytes
BlackLock
RedCurl
Gamaredon

CHINA (14)

APT10
APT41
Silk Typhoon
APT27
TRIPLESTRENGTH
Stately Taurus
Lotus Blossom
Silk Typhoon
FamousSparrow

IRAN (7)

APT73
APT73
0mid16B
APT42
MuddyWater
Cyber Av3ngers

NORTH KOREA (12)

APT38
APT45
APT43
APT37
ScarCruft

PALESTINE (5)

Handala

PAKISTAN (1)

APT-C-35

UNKNOWN (150)

RansomHub
Hunters International
Everest
FOG
Hellcat
ThreeAM
Cyber Alliance Group
CoreInjection
Safepay
GHNA
EncryptHub
UNC5337
Abyss
8Base
Natohub
Lynx Group
Babuk
IntelBroker
Money Message
Monti
Nitrogen
Codefinger
Zodiac Killer
PureCrypter
b0nd
Valerie
Emirking
INC
Crazy Hunter
Play
Tooda
Lynx
Rhysida
Brain cipher
ExploitWhispers
Stargazer Goblin
InterLock
RansomHouse
Dark Storm Team
Anonymous
Hacker collective
Arkana Security
rose87168
Weyhro

MALAYSIA (3)

DragonForce

Figure 16. Map and Number of entries by threat actors per country — Q1 2025

MOST ACTIVE

Involved in **44** activities

FOG
Ransomware Group

Threat Actors

Key Insights and recommendations

Diverse Targeting Across Sectors and Geographies

Cyber threats surged in both volume and complexity during the first quarter of 2025. From relentless ransomware campaigns to strategic state-backed intrusions, the global cyber arena is more fragmented and volatile than ever. With 40 ransomware groups, 19 APTs, and numerous hacktivist and criminal organizations active across multiple continents, Q1 reflected a shift toward hybrid threats and harder-to-trace operations.

Russia, China, North Korea, and Iran continued to drive state-aligned activity, while ransomware groups, often cloaked in anonymity, dominated the criminal sphere.

New Threat Actors

Belsen Group

Belsen Group is a new cyber threat actor that gained attention for leaking sensitive data from over 15,000 Fortinet FortiGate VPN devices, exposing numerous organizations worldwide to security risks.

Yellow Drift

Is a hacktivist group aligned with Ukraine. Their most notable activity to date is the large-scale, destructive cyber operation against Roseltorg in January 2025, stealing and wiping hundreds of terabytes of strategic data to impede critical infrastructure.

State-Sponsored Dominance in Espionage & APTs

Russia-linked actors (e.g. NoName057(16) APT28,)

Highly active (89 recorded campaigns/major activities), focusing on disruption and espionage against government, defense, and research sectors adapting TTPs to maintain persistence

China-linked actors (e.g., APT10, APT27)

Intermediate operational activities (14 campaigns/major activities), primarily targeting government, technology, and critical infrastructure

Iran-linked actors (e.g., APT42, 0mid16B)

With 7 campaigns/major activities, continued to engage in espionage, disruptive attacks, and information operations, often targeting Middle Eastern rivals and Western nations

North Korea-linked actors (e.g., APT38, ScarCruft)

12 campaigns/major activities were heavily involved in financially motivated cybercrime, targeting crypto exchanges and financial institutions.

What Q1 2025 Tells Us About What's Ahead: The start of 2025 confirms that cyber conflict is no longer confined to isolated incidents, it's a continuous and borderless phenomenon. The rise of hybrid attacks, malware recycling, and untraceable infrastructure points to a maturing threat ecosystem. FOG's rapid ascent, increased hacktivism, and mounting pressure on healthcare and defense sectors underscore an urgent need for adaptable defenses and global coordination. As lines blur between state and criminal actors, understanding the who, how, and why behind each campaign is more critical than ever.

Threats

Malware

Cyber threats analyzed in early 2025 has been shaped by a surge in infostealers, trojans, botnets, ransomware, and stealthy rootkits. Infostealers, such as **Lumma Stealer**, **Vidar**, **Redline**, and **Raccoon**, dominated the scene, with campaigns often relying on phishing, fake software updates, and malicious advertisements to harvest credentials, session cookies, and financial data. Trojans like **Njrat**, **Gh0st RAT, Quasar RAT**, and **Dark Crystal** were frequently observed acting as remote access backdoors or payload droppers for further malware, while spyware families including **Sosano**, **Backstab**, and **Desert Dexter** silently monitored victims for sensitive data extraction. Botnets, including **Murdoc, QakBot, PolarEdge**, and **Mirai**, continued to evolve, enabling large-scale DDoS attacks, spam distribution, and proxy-for-hire schemes through hijacked IoT devices and routers. **Ransomware** operations also remained active, with families like **BlackLock**, **VanHelsing**, **Albabat**, and **EncryptRAT** leveraging phishing and exploit kits to encrypt systems and demand payment. Meanwhile, **rootkits** such as **IOCONTROL**, **SPAWNCHIMERA**, and **ReaderUpdate** illustrate how attackers are adopting advanced techniques to maintain persistence and evade detection.

Top Malware

8 Entries

Lumma Stealer

A powerful and actively developed info-stealing malware designed to harvest sensitive data from infected systems and exfiltrate it to attacker-controlled servers.

4 Entries

Vidar

3 Entries

Redline

2 Entries

Gh0st RAT
XMRig
FormBook
Amos
Agent Tesla
Snake
SPAWNCHIMERA
BlackLock
GhostSocks
Dark Crystal
BADBOX 2.0
Njrat
AsyncRAT
Albabat
FogDoor
SvcStealer

NEW MALWARE

Sosano **Type:** Spyware

Description: Sosano is a lesser-known but active stealer and spyware trojan often spread through phishing campaigns, malicious loaders, or cracked software. It targets personal and sensitive information from infected Windows systems.

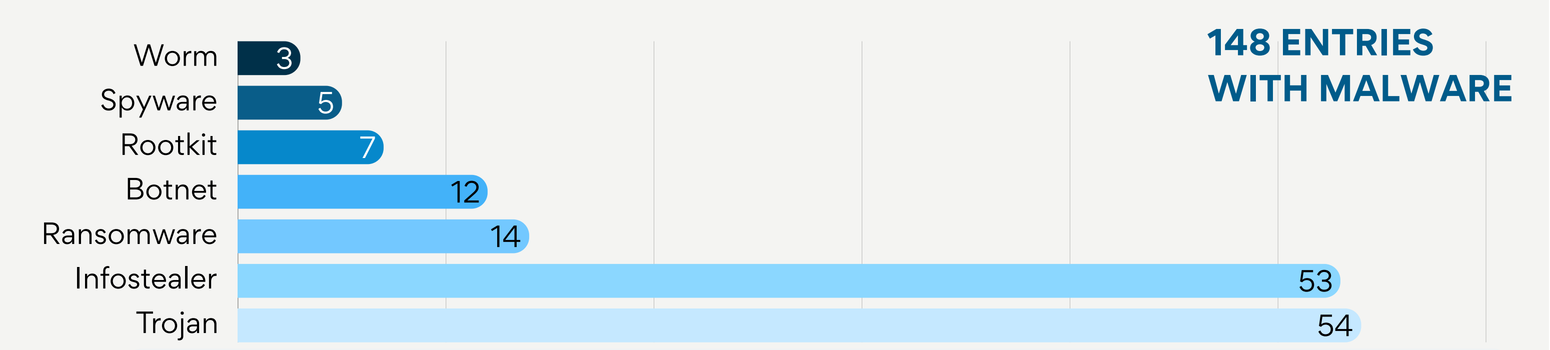
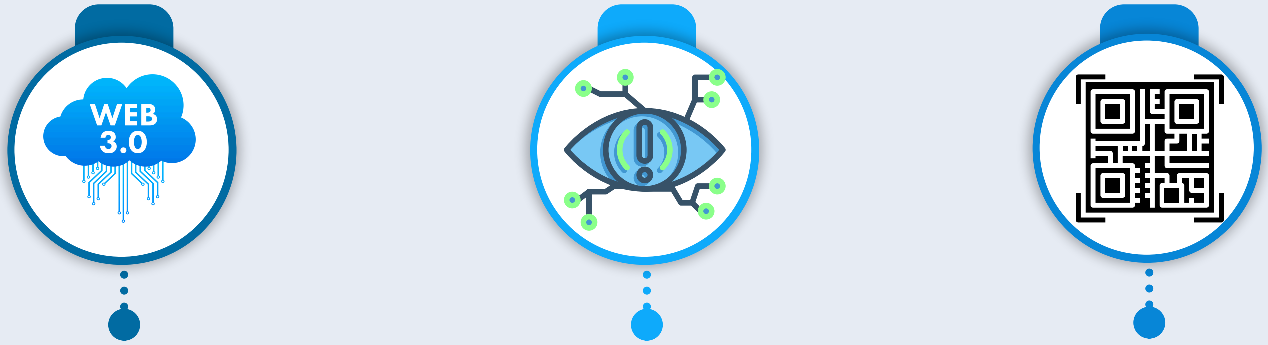


Figure 17. Amount of type of Malware per 148 entries — Q1 2025

Threats

Malicious Campaigns



OPERATION 99

Lazarus Group Targets Web3 Developers to Steal Cryptocurrency and Data

ISLAMIC REVOLUTIONARY GUARD CORPS

Iran-Linked Hackers Target UAE Organizations with New Sosano Malware Campaign

QUISHING

QR Codes Targeted by New Quishing Attack to Steal Data and Deliver Malware

Figure 18. Top 3 Malicious Campaigns — Q1 2025

Over **29 ongoing malicious campaigns** have been identified in early 2025, targeting a wide range of industries and geographic regions with increasingly sophisticated techniques. Among them, the newly discovered **SysBumps campaign** exploits macOS systems running on Apple Silicon processors, demonstrating attackers' adaptation to emerging platforms. Persistent cyber espionage efforts continue against Japanese organizations, while a phishing campaign abusing CrowdStrike's branding spreads cryptocurrency miners. Social engineering attacks remain rampant, including scams posing as government officials to steal sensitive personal and financial data, and targeted phishing against California wildfire victims. Gaming communities face threats from **infostealers** on Discord, and the notorious **Lazarus Group** focuses on **Web3** developers to siphon cryptocurrency and confidential data.

Other notable campaigns highlight evolving delivery methods and wide-reaching impact. The **Lumma Stealer** features prominently, propagating through fake **CAPTCHA** campaigns affecting global industries. Ransomware gangs have innovated with Teams calls and email bombing tactics to quickly deploy malware. Phishing emails masquerading as timesheet reports or subscription payment requests distribute malware like the **Tycoon 2FA Kit** and **Lumma Stealer**, while "**quishing**" attacks use malicious QR codes to steal data. Regional threats such as the **FatBoyPanel** targeting Indian banks, Iran-linked **Sosano malware** in the UAE, and the **GrassCall campaign** preying on job seekers show the geographic diversity of these attacks. The Lazarus Group's global Operation **Phantom Circuit** further exemplifies the escalating scale and complexity of cyber threats today. These 30-plus active campaigns underscore the critical need for comprehensive cybersecurity vigilance and adaptive defense strategies.

Top Vulnerabilities

Several critical vulnerabilities across popular enterprise software platforms underscore growing risks in remote exploitation, authentication bypass, and unsafe deserialization. CVE-2024-50603 in Aviatrix Controller allows unauthenticated attackers to execute arbitrary OS commands by injecting shell metacharacters into API parameters, affecting cloud network visibility functions. Similarly, CVE-2024-54085 impacts AMI's SPx, where attackers can remotely bypass authentication via the Redfish Host Interface, exposing organizations to complete compromise of system confidentiality, integrity, and availability. Both vulnerabilities carry the maximum CVSS* score of 10, reflecting their severity and exploitability.

Other high-impact flaws include CVE-2024-57968 in Advantive VeraCore, which permits authenticated users to upload files to unintended directories, increasing exposure to malicious content or data leakage. CVE-2025-24016 presents a serious threat in Wazuh's distributed architecture, where unsafe deserialization of JSON objects enables remote code execution through the manipulation of internal exceptions. Additionally, Ivanti EPM's CVE-2024-13159 introduces an absolute path traversal vulnerability that allows unauthenticated access to sensitive data. These vulnerabilities highlight systemic weaknesses in input sanitization, file handling, and access control, stressing the urgent need for comprehensive patching and configuration hardening across critical infrastructure.

*The **CVSS** (Common Vulnerability Scoring System) is a standardized framework used to assess the severity of security vulnerabilities. It generates a Base Score ranging from 0.0 (lowest) to 10.0 (highest), which reflects the intrinsic characteristics of a vulnerability that are constant over time and across user environments.

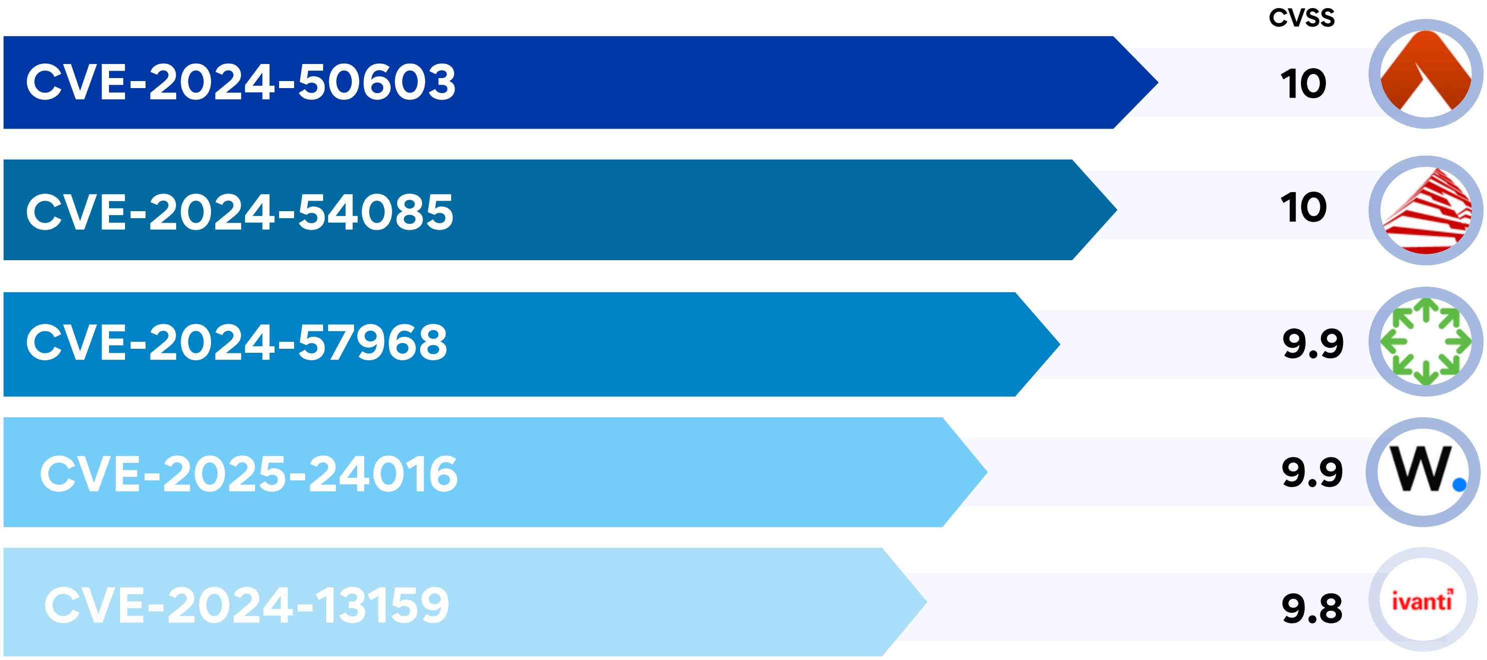


Figure 19. Top 5 Critical Vulnerabilities by CVSS Score— Q1 2025

Top Vulnerabilities

Key Insights and recommendations

ICS/OT as a Prime Target:

The leading critical vulnerabilities disclosed between January and March 2025 demonstrate a persistent trend of high-impact security flaws across diverse technology stacks—from cloud infrastructure controllers and embedded management consoles to web applications and network appliances.

Two CVEs reach the highest severity score of 10: the Aviatrix Controller (CVE-2024-50603) suffers from unauthenticated OS command injection with a strikingly high EPSS score (94.35%), signaling imminent exploitation risk; meanwhile, AMI's SPx BMC firmware (CVE-2024-54085) exposes a remote authentication bypass that threatens core confidentiality, integrity, and availability.

Other notable vulnerabilities, like the unsafe deserialization in Wazuh (CVE-2025-24016, CVSS 9.9, EPSS 91.65%) and multiple absolute path traversal flaws in Ivanti Endpoint Manager (CVEs 13159-13161, CVSS 9.8, EPSS >90%), underline common exploitation vectors rooted in inadequate input validation and access controls.

Overall, this snapshot of the top vulnerabilities emphasizes the critical need for swift patching, robust authentication mechanisms, and stringent input sanitization across enterprise environments.

Authentication bypasses remain a dominant theme, with FortiOS and FortiProxy appliances exhibiting multiple flaws (CVEs 55591, 24472) allowing attackers to gain super-admin privileges via alternate channels such as websocket modules and proxy requests.

File upload vulnerabilities in Advantive VeraCore and Apache Tomcat expose systems to arbitrary code execution or sensitive information leakage. Notably, some vulnerabilities already have public exploits available (e.g., Apache Tomcat's path equivalence flaw CVE-2025-24813), intensifying urgency for remediation.

EPSS scores vary widely, reflecting differing real-world exploit likelihoods, but several top CVEs have notably high scores above 90%, signaling elevated threat activity.

Vulnerable Vendors

In the first quarter of 2025, WordPress emerged as the most vulnerable vendor, with 517 reported Common Vulnerabilities and Exposures (CVEs). This figure significantly surpasses other major technology providers, including Microsoft (292 CVEs), Apple (266 CVEs), Linux distributions (196 CVEs), and Google (156 CVEs). The data highlights the ongoing security challenges faced by widely deployed platforms, particularly those with extensive plugin and third-party ecosystems like WordPress.

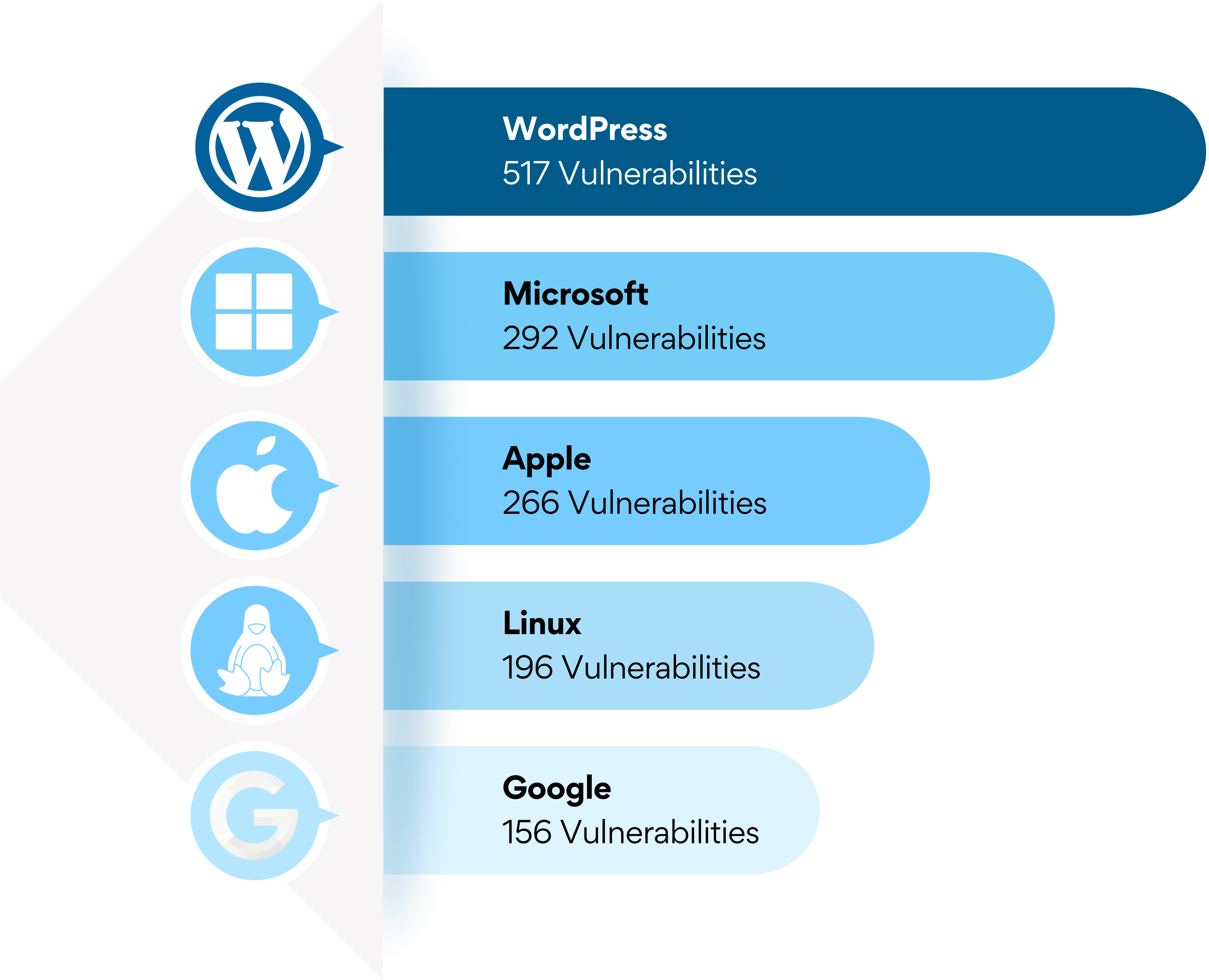
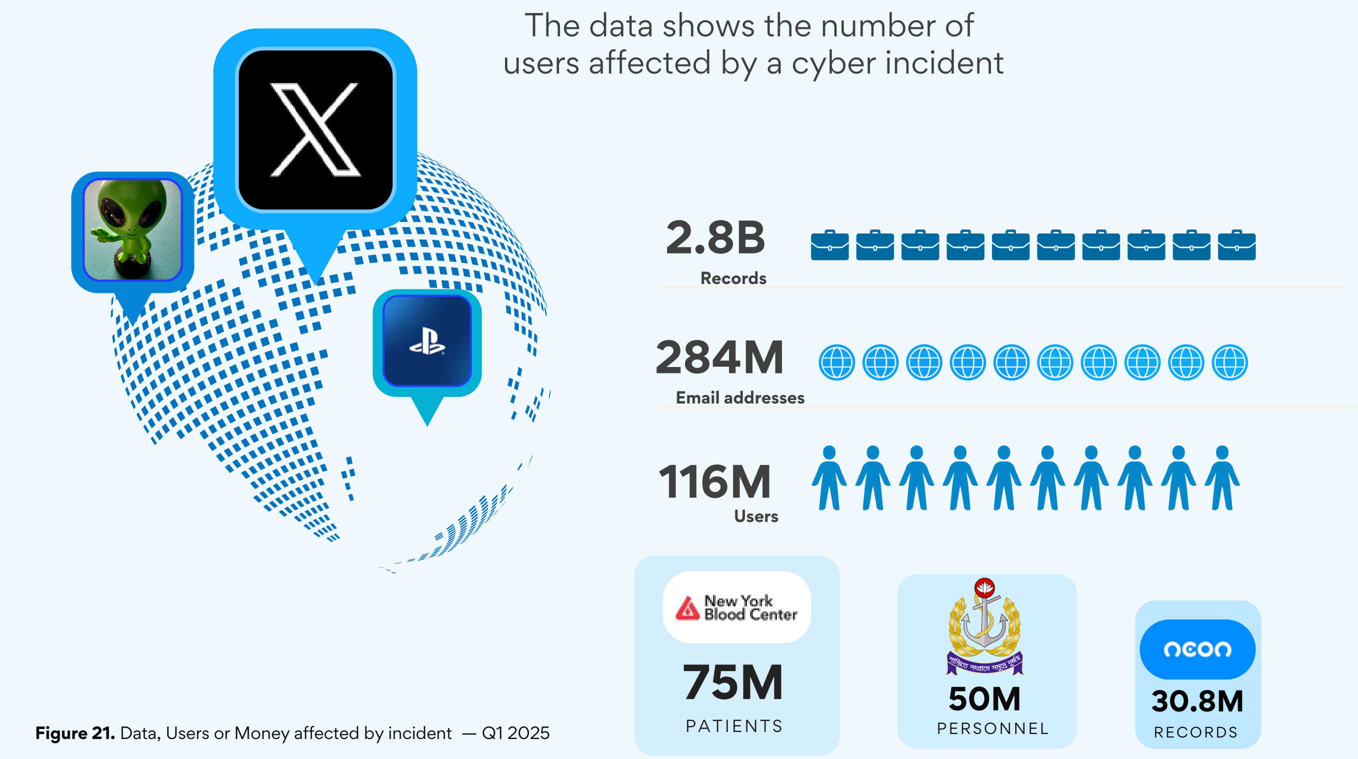


Figure 20. Top 5 Most Vulnerable Vendors — Q1 2025

Incidents Impact

Data breaches have exposed the sensitive information of billions of individuals across the globe. From tech giants like Twitter/X and Meta to healthcare providers, governments, and financial institutions, no sector has been spared. Some of the most staggering incidents include Twitter/X with nearly 2.8 billion records exposed, ALIEN TXTBASE Stealer Logs revealing 287M unique email addresses entries, and even blood donation networks like the New York Blood Center with 75 million affected. The scale and frequency of these breaches highlight just how valuable, and vulnerable, personal data has become.

While global platforms experience the largest raw numbers, the impact of smaller breaches at hospitals, schools, and local governments can be just as severe for affected individuals. Healthcare alone saw dozens of incidents, reflecting a persistent pattern of underinvestment in cybersecurity across critical services. This snapshot of recent attacks underscores the urgent need for stronger protections, faster breach response, and a collective shift toward securing the digital infrastructure we rely on daily.



The data shows the number of users affected by a cyber incident

2.8B Records

284M Email addresses

116M Users

New York Blood Center 75M PATIENTS

50M PERSONNEL

neon 30.8M RECORDS

Figure 21. Data, Users or Money affected by incident — Q1 2025

$1.5B

The largest confirmed cryptocurrency theft

Incidents Impact

Key Insights

Top 5 breaches

This quarter was marked by a few massive breaches that exposed over **3.2B** records. Incidents at Twitter/X, ALIEN TXTBASE Stealer Logs and PlayStation show how a single breach in a data-rich environment can have global impact. Even critical sectors like healthcare and national defense were hit hard, with New York Blood Center and the Bangladesh Navy among the top victims.

Ransomware as the primary weapon

Most of the major incidents analyzed this quarter were linked to ransomware attacks, where data was not only encrypted but later leaked to extort victims further. Most of the incidents followed this pattern, first paralyzing operations, then exposing sensitive data online.

The Supply Chain is a Major Vulnerability:

Several incidents highlighted the risk posed by third-party vendors. Attackers are increasingly targeting smaller, less secure partners to gain a foothold into the networks of their larger, primary targets.

“Unauthorized Access" and "System Intrusion" were recurring themes, indicating that attackers are successfully exploiting vulnerabilities like weak credentials, unpatched systems, and poorly configured cloud environments.

Record Crypto Theft

Alongside record-breaking data breaches, the quarter also saw one of the largest cryptocurrency thefts to date: Bybit lost a staggering **$1.5 billion** worth of Ethereum. This incident highlights the growing financial stakes of cybercrime, where attackers are not just stealing data, but money at scale.

Affected Industries

Analyzing the incident data reveals that the top 5 most affected sectors, in order of incident frequency, include: Government (86 incidents), Healthcare (67 incidents), Education & Research (57 incidents), Consumer Products & Retail (40 incidents), and Engineering & Industrial (39 incidents). These sectors represent the areas with the highest frequency of reported incidents within the dataset, highlighting significant vulnerabilities.

While Government leads in incident count, the impact of some breaches transcends sector boundaries and traditional incident metrics. Notably, a data exposure on Twitter/X resulted in an astonishing **2.8B records** being compromised, demonstrating the immense scale of data at risk on digital platforms. Similarly, the ALIEN TXTBASE Stealer Logs exposed **287M unique email addresses**, underscoring the widespread nature of credential theft.

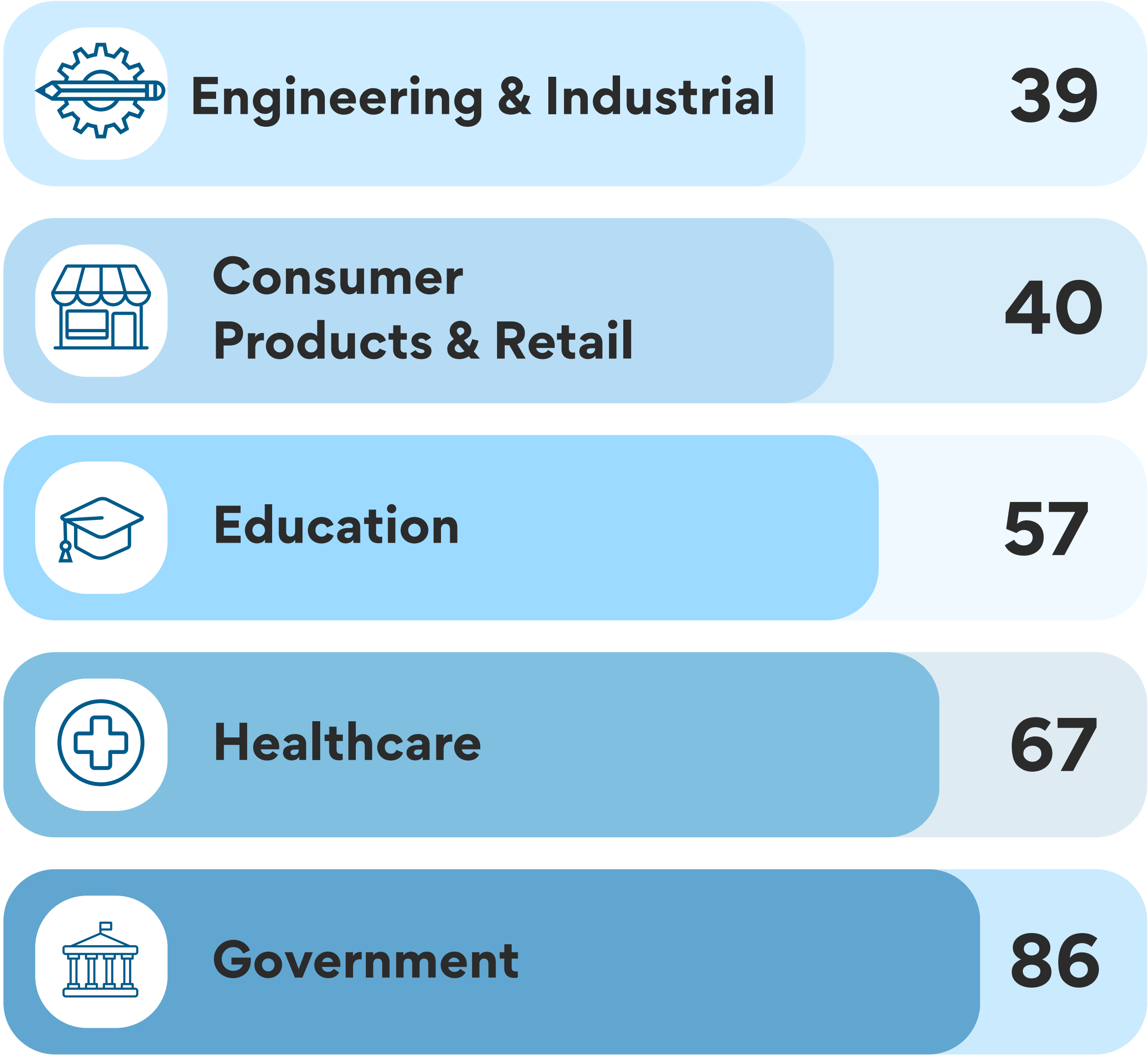


Figure 22. Amount of incidents per sector/industry — Q1 2025

Affected Industries

Key Insights by Sector

Examining the impact on individuals within these top sectors, and beyond, shows significant variation in the amount of people affected.

Blockchain & Cryptocurrency:

Bybit

In terms of financial impact, a single incident involving Bybit Blockchain led to a staggering loss of $1.5 billion, showcasing the catastrophic financial repercussions that can occur, particularly in the rapidly evolving digital currency market. These high-profile incidents serve as a stark reminder that while incident frequency is a key indicator, the sheer volume of data exposed and the financial implications can be even more devastating.

- $1.5B worth of cryptocurrency from one of its Ethereum cold (offline) wallets

Technology & Business Services:

WhatsApp

Meta confirmed a Zero-Click WhatsApp Spyware attack targeting 90 Journalists and civil society members. The campaign used a spyware from an Israeli company known as Paragon Solutions.
The people targeted own phones with numbers tied to Belgium, Greece, Latvia, Lithuania, Austria, Cyprus, Czech Republic, Denmark, Germany, the Netherlands, Portugal, Spain and Sweden.

Government:

The Most Frequent Target

The Government sector recorded the highest number of security incidents, indicating a persistent, widespread campaign by threat actors against government entities at local, state, and national levels. A notable instance of this pervasive threat is the impact on the Bangladesh Navy by the Funksec threat actor, affecting 50 million service members. While these attacks were individually smaller in some cases, their high frequency suggests a constant state of siege, draining public resources, eroding trust, and posing a continual threat to sensitive civic and defense data.

Affected Regions

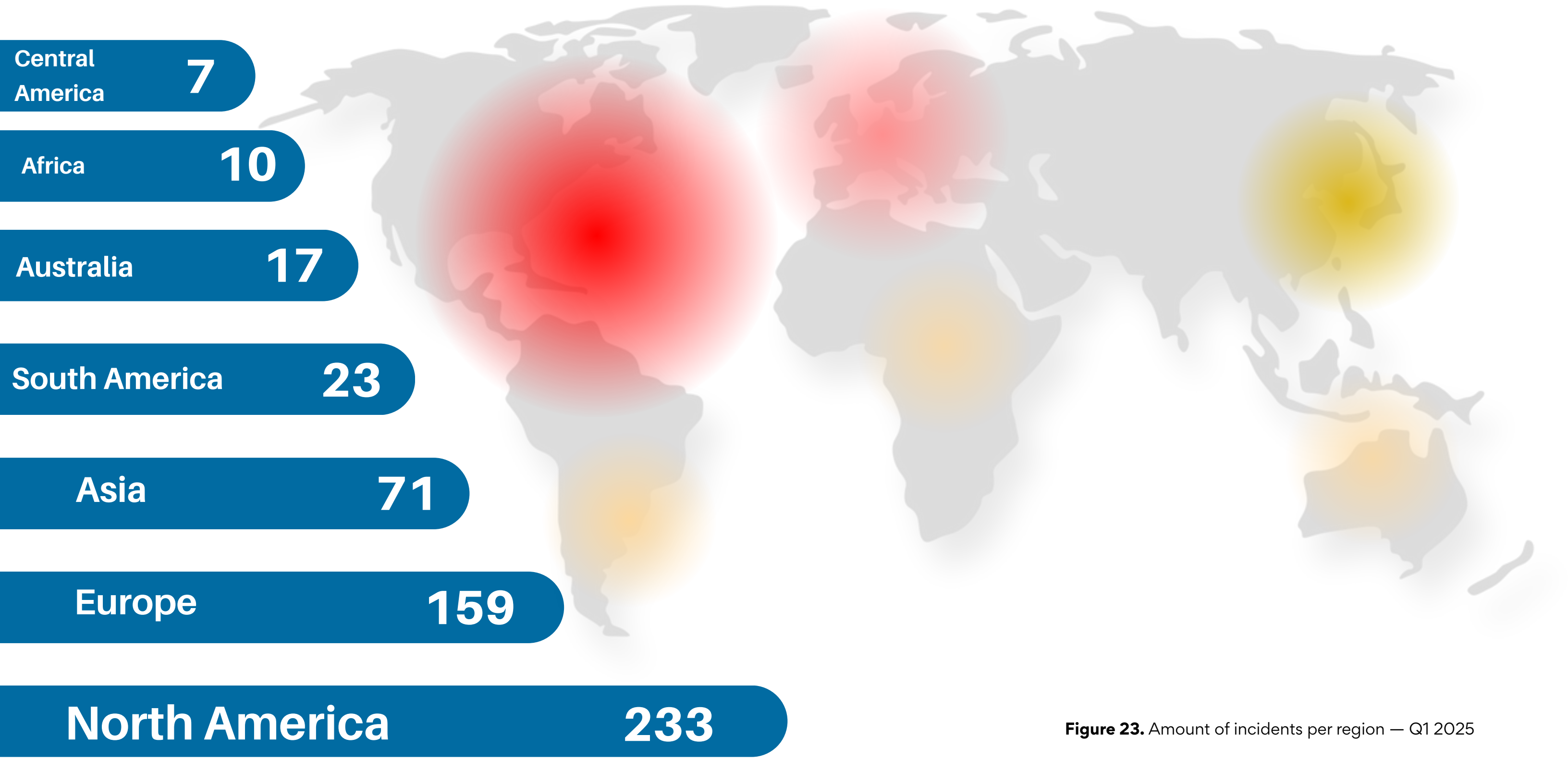


Figure 23. Amount of incidents per region — Q1 2025

Insight

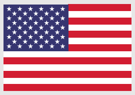
Out of the 545 entries analyzed, 25 incidents were classified as having a global impact. These incidents are significant as they are not limited to a single region and can affect multiple countries or international entities.

Looking at the country-specific data, the top 5 countries with the highest number of reported incidents during this period were the USA with 222 incidents, followed by Germany with 45, France with 20, and the UK with 17. This highlights the varying levels of incident activity experienced by different nations.

Affected Regions

Key Insights and recommendations

An analysis of the geographic locations of the organizations discussed reveals a significant concentration of incidents in North America, particularly the USA, which saw a high volume and diverse range of sector impacts. Concurrently, Europe also experienced major, high-impact breaches, exemplified by incidents in the UK and Germany.



United States as the Epicenter of Mega-Breaches

- **Healthcare** as a Primary Target: The sector appears to be disproportionately affected, with multiple incidents impacting a substantial number of individuals. Notable examples include New York Blood Center Enterprises (75M affected), Community Health Center (1M affected), and Frederick Health (934K affected).
- Education and Research Vulnerabilities: Educational institutions, from universities to school districts, are also targets. NYU, with 3M affected, and Chicago Public Schools (320K affected), are prime examples.

Significant Impact in Europe

- In Europe, significant data breaches have impacted millions across key sectors. The UK's telecommunications giant TalkTalk faced an incident affecting 18.8M individuals, similarly, in Germany, the Thermomix kitchen breach impacted 3.3M, and Germany's Mercury Group saw 1M individuals affected.
- These 3 incidents collectively represent a significant impact on European citizens, affecting millions of individuals. They serve as a stark reminder that regardless of the industry, organizations handling personal data are prime targets.

Recommendations

- **Robust Encryption:** Implement strong, end-to-end encryption for data both at rest (stored) and in transit (being transmitted). This ensures that even if data is breached, it remains unreadable and unusable to unauthorized parties.
- **Harmonize Global Incident Response:** Develop a unified incident response plan that can be localized. This plan must include legal counsel familiar with the breach notification laws in every country where you have customers to ensure compliant and timely reporting on a global scale.
- **Regular Software Updates and Patch Management:** Keep all operating systems, applications, and firmware updated with the latest security patches to address known vulnerabilities that attackers frequently exploit. Automate updates where possible.

Civil Judicial Actions

A review of recent data breach settlements and enforcement actions reveals increasing regulatory pressure and financial consequences for organizations failing to implement basic cybersecurity and privacy safeguards. Multiple companies, including healthcare providers, financial institutions, and tech firms, faced regulatory action by U.S. agencies such as the HHS OCR, SEC, and FTC, as well as international regulators like the AEPD (Spain) and UODO (Poland). Common violations included failure to conduct risk assessments, insufficient breach notifications, unauthorized data disclosures, and deceptive practices. Penalties ranged from tens of thousands to multi-million-dollar settlements, with some cases resulting in corrective action plans spanning several years. Notably, **Solara Medical Supplies** paid **$3 million** for HIPAA violations, **PayPal** was fined **$2 million** for access control failures, and **Cognosphere** settled for **$20 million** due to COPPA and deceptive practices.

In parallel, class action lawsuits against companies like **UnitedHealth**, **MGM Resorts**, **Harvard Pilgrim**, and **Infosys McCamish** underscored the financial and reputational risks of inadequate cybersecurity. These civil actions, often triggered by ransomware attacks or misconfigured systems, alleged negligence, breach of contract, and privacy violations. Settlements frequently included substantial monetary compensation, identity theft protection, credit monitoring, and commitments to improve data security. The largest of these included a **$45 million** settlement by **MGM Resorts** and a **$17.5 million** proposed fund by **Infosys McCamish**. The trends point to a regulatory and legal environment that increasingly holds organizations accountable for data protection failures, particularly where sensitive health or financial information is involved.

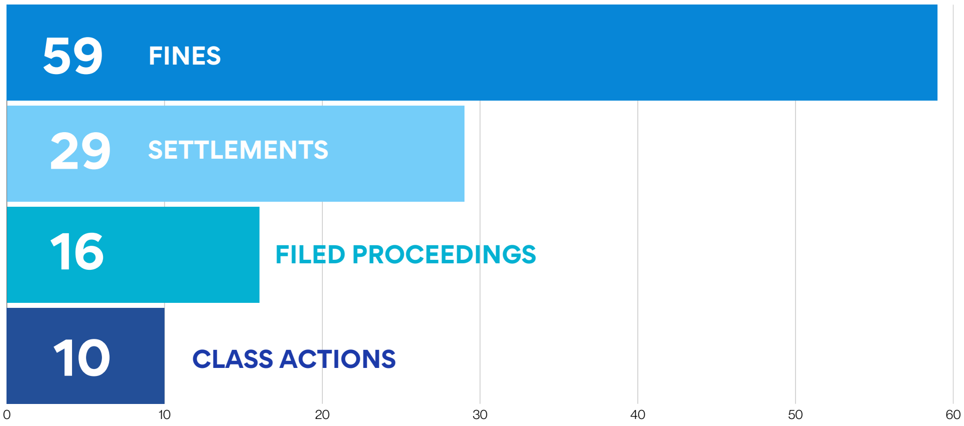


Figure 24. Amount of Civil Judicial Actions Per Category— Q1 2025

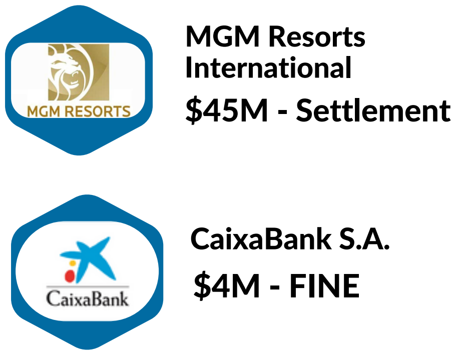


Figure 25. Top 2 Settlement/Fine — Q1 2025

Civil Judicial Actions

Key Insights

Regulatory Enforcement Is Escalating:

- Agencies like the HHS OCR, SEC, FTC, and international counterparts are increasingly imposing significant fines and long-term corrective actions.
- Violations often stem from basic lapses such as not performing risk assessments, delayed or incomplete breach notifications, or lack of access controls.

☑ Deceptive Practices Are a Major Focus:

Firms misrepresenting their data security or privacy practices, especially to children or vulnerable populations, are being penalized heavily (e.g., Cognosphere/COPPA case).

☑ Healthcare and Financial Sectors Are High-Risk Targets:

Most enforcement actions and class action lawsuits involve health and financial data, indicating these sectors face elevated scrutiny due to the sensitivity of the data they handle.

Cyber Trends

Figure 26. World Cloud of Key Terms — Q1 2025

Conclusion

The first quarter of 2025 vividly illustrates that cybersecurity remains a high-stakes arena shaped by opportunity, risk, and consequence; a battleground defined by The Good, The Bad, and The Ugly.

The Good shows that strategic investments, policy innovation, and coordinated law enforcement are strengthening global cyber defenses. Organizations that adopt managed security services, embrace proactive threat detection, and align with emerging regulatory frameworks are better positioned to resist attacks.

The Bad underscores the unrelenting rise of cyber threats. Ransomware gangs, APTs, and infostealer malware exploited critical vulnerabilities at an unprecedented scale. The surge in CVEs and malicious campaigns illustrates that attackers are faster, more adaptive, and increasingly hybrid in their operations.

The Ugly highlights the tangible damage of cyber incidents: multi-billion-dollar cryptocurrency thefts, historic data breaches, and cascading operational disruptions across essential industries. The financial, reputational, and legal consequences are now unavoidable for organizations without robust defenses.

Moving forward, the key to resilience lies in intelligence-driven security, rapid vulnerability management, cross-sector collaboration, and continuous investment in cybersecurity. In a world where threats evolve daily, preparedness is not just a defensive measure, it is a strategic imperative for survival.

Methodology

This **Hall of Hacks** report provides a comprehensive overview of the Q1 2025 cybersecurity field by analyzing data harvested from diverse, reputable sources. Our methodology involves two key phases: **data harvesting** and **analytical processing**.

Data Harvesting: We collect information from public and private cybersecurity intelligence feeds, industry reports, and news outlets. This includes tracking CVEs from vulnerability databases, monitoring active threat actors, and gathering details on incidents, financial investments, legal actions, and malware strains.

Analytical Processing: The collected data undergoes rigorous analysis, which includes: Quantitative Analysis: We apply statistical methods to quantify various aspects of the cybersecurity domain, such as the total number of incidents, CVEs, and the financial impact of legal actions.

Categorization and Classification: Incidents, threat actors, malware, and vulnerabilities are classified by type, origin, target, and impact.

Trend Identification: We perform longitudinal analysis to identify emerging trends in cyber threats, investments, and policy shifts.

Impact Assessment: The impact of incidents is assessed based on the number of affected individuals, monetary losses, and operational disruptions.

Geographical Mapping: Data is mapped geographically to highlight affected regions, countries, and investment and M&A activities.

Expert Review: All findings are subjected to expert review for accuracy and contextual understanding.

This robust approach ensures a clear, accurate, and actionable understanding of the Q1 2025 cybersecurity environment.

Sources:

Glossary

APT (Advanced Persistent Threat):

A stealthy, prolonged cyberattack where a threat actor gains unauthorized access to a network and remains undetected to exfiltrate data or conduct espionage.

Botnet:

A network of compromised devices controlled remotely by attackers, often used for DDoS attacks, spam, or malware distribution.

Campaign (Malicious Campaign):

A coordinated series of cyberattacks targeting specific organizations, sectors, or regions over a period of time.

Cloud Security:

Practices, technologies, and policies designed to protect cloud-based data, applications, and services from threats and breaches.

Credential Theft:

The unauthorized acquisition of usernames, passwords, or other authentication information, typically used for account compromise.

Critical Vulnerability:

A security flaw with a high or maximum CVSS score that can be easily exploited to cause significant impact on confidentiality, integrity, or availability.

Crypto Theft (Cryptocurrency Theft):

The illegal acquisition of digital currency, often via exchange breaches, wallet compromises, or phishing campaigns targeting Web3 users.

CVEs (Common Vulnerabilities and Exposures):

A standardized identifier for publicly disclosed software and hardware security vulnerabilities.

CVSS (Common Vulnerability Scoring System):

A standardized framework for rating the severity of software vulnerabilities, with scores from 0 (lowest) to 10 (highest).

Data Breach:

An incident where sensitive, protected, or confidential data is accessed, disclosed, or stolen by unauthorized parties.

EPSS (Exploit Prediction Scoring System):

A system that estimates the likelihood a given vulnerability will be exploited in the real world.

Glossary

Exploit Kit:

A collection of automated tools designed to exploit known software vulnerabilities to deliver malware to victims.

Hacktivist:

An individual or group conducting cyberattacks to promote political or social agendas rather than financial gain.

Incident:

A confirmed cybersecurity event that compromises information, systems, or networks.

Infostealer (Information Stealer):

Malware designed to harvest credentials, session cookies, financial data, and other sensitive information from infected devices.

Law Enforcement Action (Criminal Judicial Action):

Activities such as arrests, indictments, extraditions, and convictions targeting cybercriminals or threat actors.

Malware:

Any malicious software intended to harm, exploit, or disrupt computer systems, including viruses, worms, trojans, spyware, and ransomware.

Managed Security Services (MSS):

Outsourced services that monitor, manage, and respond to cybersecurity incidents on behalf of organizations.

M&A (Mergers and Acquisitions):

Business transactions where one company acquires another or merges with it, relevant in cybersecurity when companies consolidate capabilities.

Patch Management:

The process of regularly updating and fixing software vulnerabilities to prevent exploitation.

Phishing / Quishing:

Deceptive attempts to trick users into revealing sensitive information. Quishing refers to phishing attacks using QR codes.

Ransomware:

Malware that encrypts a victim’s data and demands payment (ransom) for the decryption key.

Glossary

Rootkit:

Malicious software designed to hide its presence and maintain privileged access to a computer system.

Sector / Industry Impact:

Analysis of which industries—such as healthcare, government, or education—are most affected by cyber incidents.

Spyware:

Malware that secretly observes user activity, collecting data such as keystrokes, screen captures, or communications.

Supply Chain Attack:

A cyberattack targeting less secure third-party vendors to gain access to larger organizations' networks.

Threat Actor:

An individual or group responsible for malicious cyber activity, including state-sponsored groups, cybercriminals, and hacktivists.

Threat Landscape:

The overall environment and trends of current cyber threats, including active groups, malware, and vulnerabilities.

Trojan (Trojan Horse):

Malware disguised as legitimate software to trick users into installing it, often used as a delivery mechanism for other threats.

Vulnerability:

A flaw or weakness in software, hardware, or configurations that could be exploited to compromise security.

WordPress Vulnerabilities:

Security flaws in the WordPress CMS or its plugins/themes, which are frequent targets due to the platform's popularity and open ecosystem.

CYBERMATERIAL

Prepared by:
Sofia V.
Marc R.
Nicolas P.

hello@cybermaterial.com

cybermaterial.com/hall-of-hacks

Powered by

911 CYBER

https://911cyber.app

Hall of Hacks