



HALL OF HACKS

Q4 - 2024

Prepared by



Powered by



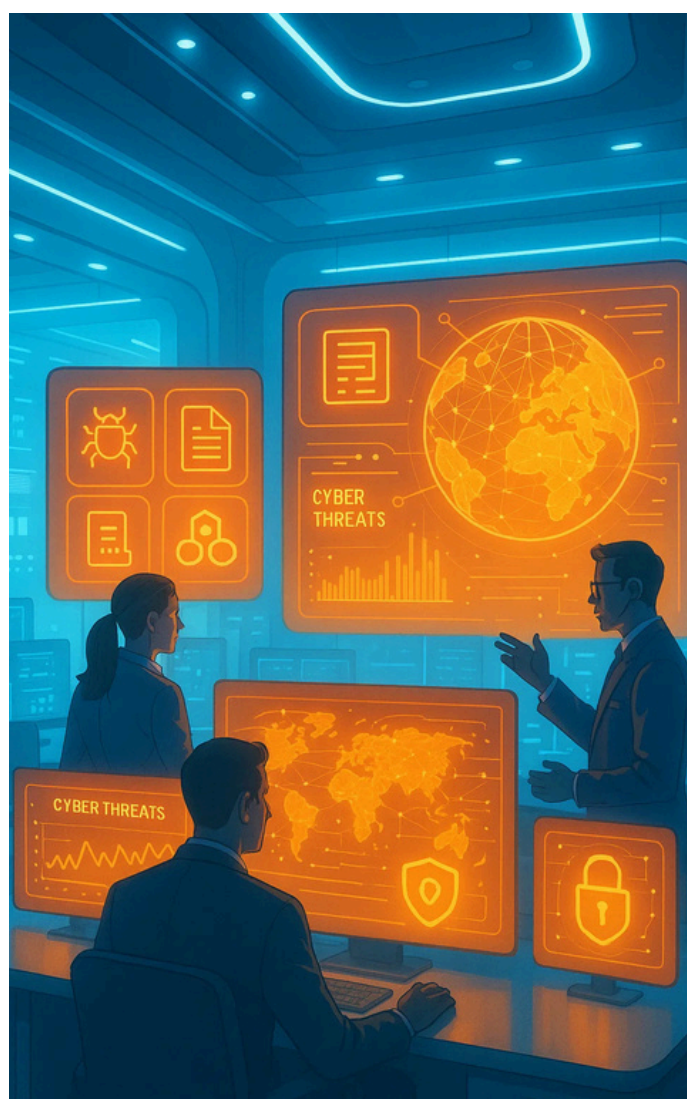


Table of Contents

03	Introduction	07	The Good
04	Executive Summary	14	The Bad
05	Inductees	24	The Ugly
06	Findings	33	Conclusion

Introduction

The Q4 2024 Hall of Hacks report by CyberMaterial in partnership with 911Cyber provides an in-depth analysis of the cybersecurity landscape from October to December 2024.



This quarter's report categorizes key events and figures into "The Good," "The Bad," and "The Ugly" to provide a nuanced perspective. "The Good" highlights positive developments such as top investments in cybersecurity firms like Cyera (Top Investment) and significant mergers and acquisitions, including Darktrace (Top M&A), alongside important cyber policy advancements like the UN Cybercrime Convention (Top Cyber Policy). "The Bad" focuses on negative elements, notably the activity of threat actors like APT29 (Top Threat Actor), the prevalence of threats such as Sarcoma (Top Threat), and critical vulnerabilities, for example, in ABB products (Top Vulnerability). "The Ugly" details the most detrimental incidents and outcomes, including Change Healthcare becoming the Top Victim of a cyberattack, Government being the Most Affected Industry, and significant legal actions such as the sentencing of Roman Sterlingov (Top Judicial Action) and the hefty fine imposed on Meta (Top Legal Action).

Furthermore, the report emphasizes the interconnectedness of the various elements within the cybersecurity ecosystem. From the technical details of malware and vulnerabilities to the broader implications of legal and policy developments, the analysis illustrates how each component influences and is influenced by the others. By synthesizing this information, the Hall of Hacks Q4 2024 report delivers actionable intelligence for security practitioners, policymakers, and business leaders seeking to navigate and mitigate the multifaceted risks present in today's digital environment.

Executive Summary

The Q4 2024 cybersecurity landscape was characterized by a high volume of cyber threats and evolving tactics. Key findings include 478 recorded incidents, the identification of 119 active threat actors, and the operation of 31 ransomware groups. The quarter also saw 3,750 Common Vulnerabilities and Exposures (CVEs) disclosed and 110 malware strains in active circulation.

Financially, the cybersecurity sector witnessed significant investment momentum, with major funding rounds for companies like Cyera, Armis, Halcyon, and Upwind, and continued early-stage funding activity. Mergers and Acquisitions were also prominent, particularly in the Managed Security Services Provider (MSSP) sector.

In terms of threats, ransomware and trojans remained prevalent, with new malware strains like BianLian emerging. Vulnerabilities were a major concern, with ABB and Cleo products identified as having critical flaws. The most vulnerable vendor was Microsoft, with 587 reported vulnerabilities. Several high-impact incidents affected millions of individuals, with Change Healthcare suffering a ransomware attack that impacted 190 million people. The most affected industries were Government and Healthcare.

Law enforcement agencies were active in pursuing cybercriminals, with numerous arrests and asset seizures. Legal actions also resulted in substantial financial penalties. Overall, the report highlights the need for organizations to prioritize proactive defense, threat intelligence, and adaptive security strategies to effectively counter the evolving threat landscape.

Inductees

Top Investment



cyera
\$300M

Top M&A



Darktrace
by ThomaBravo
\$5.6B

Top Regulation



**UN Cybercrime
Convention**
Agreement

Top Judicial Action



Roman Sterlingov
Operated Bitcoin Fog
Sentenced

Top Threat Actor



APT29
Most Active

Top Threat



Sarcoma
Most Active

Top Vulnerability



CVE-2024-51551
Highest CVSS score

Most Vulnerable Vendor



Microsoft
Most CVEs

Top Victim



Change Healthcare
190M people

Most Affected Industry



Government
Most Incidents

Most Affected Country



USA
Most Targeted

Top Legal Action



META
\$280M FINE

Findings

Highlights



During Q4 2024, the cybersecurity landscape remained highly active, with a total of 478 recorded incidents. Threat intelligence identified 18 ongoing malicious campaigns and activity from 119 threat actors, including 22 advanced persistent threat (APT) groups. A notable 31 ransomware groups were operational during the quarter, contributing to widespread disruption across sectors. In addition, 3,750 Common Vulnerabilities and Exposures (CVEs) were disclosed, highlighting the persistent challenge of vulnerability management. The period also saw 110 malware strains in active circulation. These findings underscore the increasing complexity and volume of global cyber threats.



Incidents
478



Malicious Campaigns
18



CVEs
3750



Active Threat Actors
119



APTs
22



Ransomware Groups
31



Active Malware
110



New Malware
5

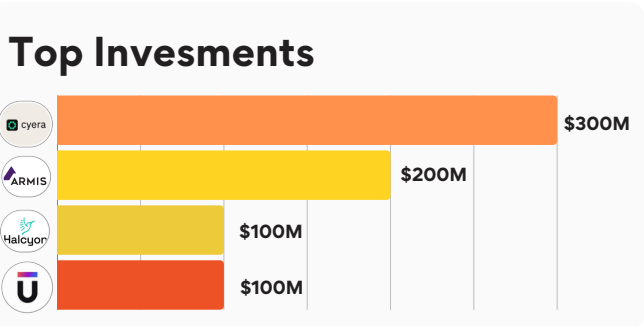
Financing

Funding

The final quarter of 2024 showcased strong momentum in cybersecurity investments, with both large-scale funding rounds and a surge in early-stage activity. Four standout investments led the period: Cyera raised \$300 million in a Series D round (Data Protection), Armis secured \$200 million (Asset Visibility & Security), Halcyon attracted \$100 million (Ransomware Prevention), and Upwind also closed \$100 million in Series B funding (Cloud Security). These highlight sustained investor confidence in mature companies tackling critical security challenges.

Total Investments

54



● Highlights

A steady stream of Seed and Series A rounds, backing startups like System Two Security, NetBird, and Prime Security, underscored a healthy pipeline of innovation.

Most funding rounds were concentrated in the USA, with a focus on Series A, B, and C rounds. Several companies from Israel and France also raised capital, including Zenity (Israel, Series B) with \$38M and Filigran (France, Series B) with \$35M. There is also a notable focus on Seed funding rounds, with a variety of companies from across the globe, such as Symbiotic Security (USA, Seed) and Prompt Security (Israel, Series A).

Early-stage funding remained robust, especially in Threat Detection & Response, Managed Security Services, and Governance, Risk & Compliance (GRC).



Financing

Mergers & Acquisitions

Surge in MSSP Deals: Managed Security Services (MSS) continued to dominate M&A activity across all three months, reflecting enterprise demand for outsourced security capabilities.

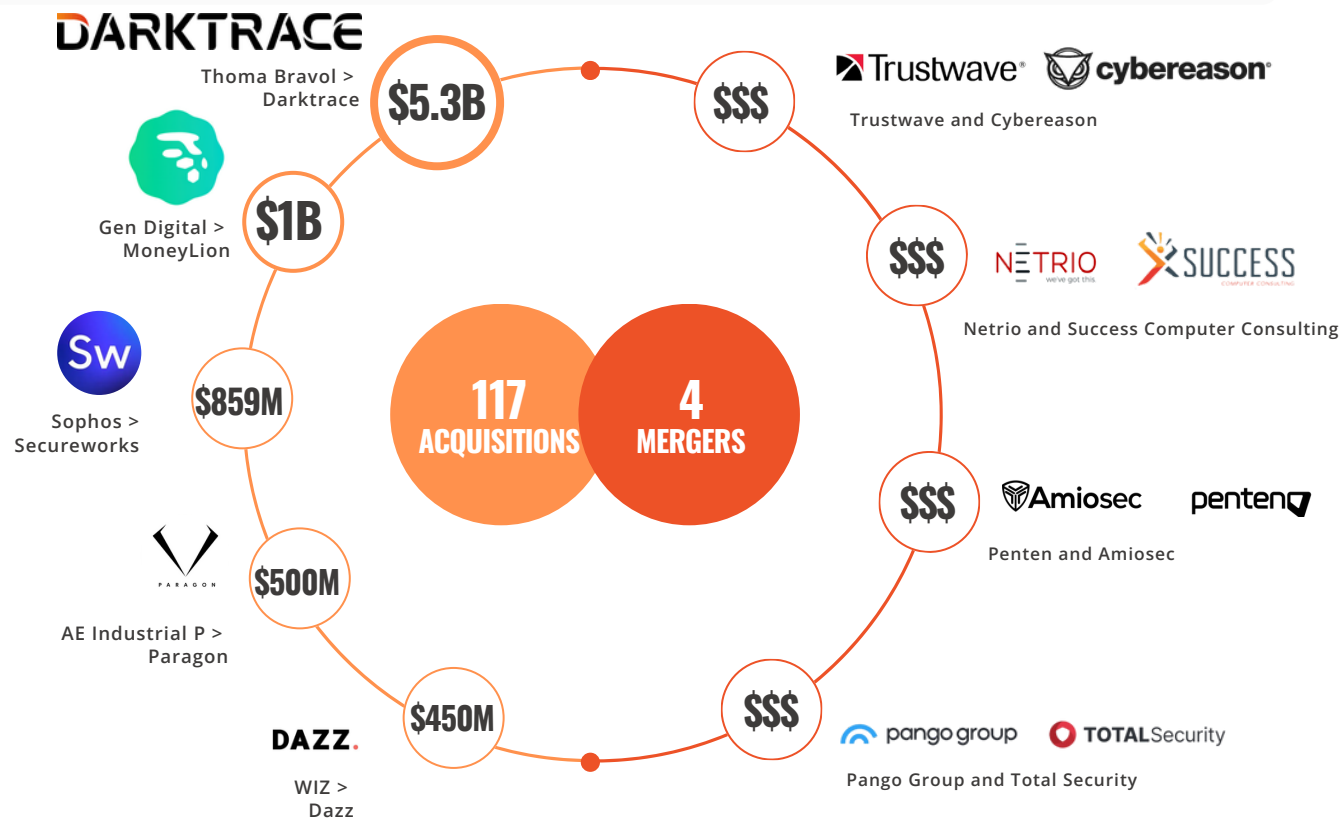
Cloud and Threat Detection: High-value deals were observed in cloud security and threat detection & response, highlighting strategic investment in proactive defense and remote infrastructure protection.

Geographical Spread: The U.S. led global cybersecurity M&A, followed by strong activity in the UK, Australia, Germany, and Israel.

Sector	#Deals
Managed Security Services (MSS)	36
Threat Detection & Response	18
Network & Infrastructure Security	11
Cloud Security	10
Identity and Access Management (IAM)	6
Governance, Risk & Compliance (GRC)	6
Data Protection / Security	6
Application & Software Security	5
Security Awareness & Training	5

Total M&A : 121

Aquisition Merger



Financing

Key Insights, forecast and recommendations

Insights:



- Q4 2024 showed strong cybersecurity investment, with 54 total investments. Top funding went to Data Protection (\$300M - Cyera), Asset Visibility & Security (\$200M - Armis), Ransomware Prevention (\$100M - Halcyon), and Cloud Security (\$100M - Upwind). Early-stage funding was robust in Threat Detection & Response, Managed Security Services (MSS), and GRC. The USA led funding, with activity also in Israel and France.
- Mergers & Acquisitions (M&A) surged with 121 deals (117 acquisitions, 4 mergers). MSS dominated M&A with 36 deals, followed by Threat Detection & Response (18) and Network & Infrastructure Security (11). High-value deals were seen in cloud security and threat detection. The U.S. led global M&A, with strong activity in the UK, Australia, Germany, and Israel.

Forecast:



Looking ahead, the cybersecurity market is expected to maintain its robust growth trajectory.

- Sustained Investment: Investor confidence in addressing critical security challenges is likely to continue, driving sustained investment in both mature and early-stage companies.
- Consolidation in Key Segments: The high volume of M&A, particularly in Managed Security Services, suggests ongoing consolidation as larger players seek to integrate specialized capabilities and expand their service offerings. This trend is also likely to continue in Cloud Security and Threat Detection & Response.
- Geographic Expansion: While the USA will likely remain the dominant market, increased cross-border investment and M&A activity, particularly with companies in the UK, Australia, Germany, Israel, and France, is anticipated as global security needs become more interconnected.
- Focus on Emerging Threats: As the threat landscape evolves, expect continued investment in solutions addressing new and emerging threats, potentially leading to new categories of cybersecurity funding beyond the currently dominant ones.

Recommendations for Stakeholders:



- Investors should focus on high-demand areas like Data Protection, Cloud Security, Threat Detection & Response, and MSS, both for early-stage and M&A opportunities.
- Cybersecurity Startups focus your solutions on Data Protection, Cloud Security, Ransomware Prevention, or Asset Visibility & Security to attract significant investment.
- Established companies should pursue strategic acquisitions and capitalize on the active M&A market to acquire innovative companies, especially in MSS, Cloud Security, and Threat Detection & Response, to expand capabilities.

Cyber Policies

41

Q4 New Policies

Cybersecurity policy activity slowed in Q4 2024, with 41 new laws, regulations, amendments, agreements, bills, executive order and guidelines recorded. Legislative attention remained focused on critical domains such as NIS2 Directive transpositions, AI system security, and data protection. The reduced volume suggests a shift from broad expansion to more focused regulatory refinement, as governments and institutions begin operationalizing the wave of policies introduced earlier in the year.

Focusing on Regulatory Transposition, Data Governance, and Financial Security

11 Regulations

9 Amendments

6 Laws

6 Bills

5 Guidelines

3 Executive Order

1 Agreements



● Highlights

Q4 2024 showcased significant regional activity, with Europe and North America leading the charge on cybersecurity legislation. The EU continued its commitment to the NIS2 Directive transposition, with multiple member states enacting or amending regulations, reflecting the region's ongoing efforts to strengthen cybersecurity frameworks across sectors. In North America, the U.S. introduced executive orders and amendments to enhance security for critical infrastructure and personal data, while Canada and other nations like Lithuania emphasized national cybersecurity laws. This geographical distribution signals a growing global alignment on cybersecurity priorities, with particular emphasis on financial sector protections, critical infrastructure resilience, and data governance.

Cyber Policies

Recommendations for Stakeholders

For Legal & Compliance Teams:

Continuous Regulatory Monitoring: Establish or enhance mechanisms for proactively monitoring new and updated cyber laws, regulations, and guidelines, especially in jurisdictions where the organization operates or plans to operate.

For Cybersecurity & IT Operations Teams

Prioritize Implementation of New Mandates. Strengthen incident reporting capabilities, utilize 'Guidelines' and 'Executive Orders' as valuable sources of cybersecurity best practices and governmental priorities to enhance existing cybersecurity frameworks

For Executive Leadership & Board of Directors

Strategic Investment in GRC Tools, allocate adequate resources, include cybersecurity policy compliance as a regular agenda item in board and executive risk review meetings.

Agreement

UN Cybercrime Convention



193
UN members

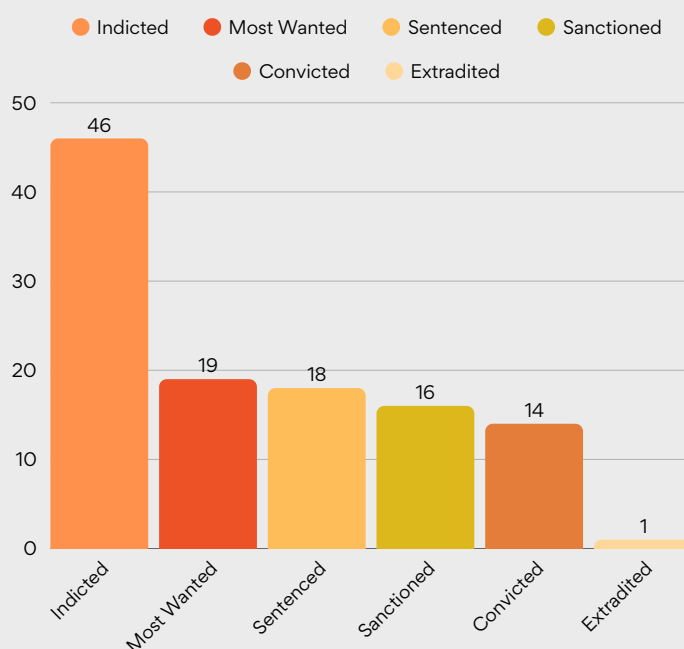
UN General Assembly adopts milestone cybercrime treaty.

The General Assembly adopted the United Nations Convention against Cybercrime, a landmark global treaty aimed at strengthening international cooperation to combat cybercrime and protecting societies from digital threats.

Criminal Judicial Actions

Law enforcement across the US, UK, EU, and INTERPOL coordinated extensive operations targeting ransomware actors, dark web marketplaces, and fraud rings. This included INTERPOL's record-setting 5,500 arrests and \$400 million in asset seizures, along with multiple U.S. Department of Justice cases targeting individuals engaged in phishing, identity theft, cryptojacking, and online extortion.

6,565
Arrests



SENTENCED



12 YEARS

ROMAN STERLINGOV
OPERATED BITCOIN FOG



The most notorious groups featured prominently in these actions include LockBit, Evil Corp, and APT27. **LockBit's** developer and affiliates were arrested or indicted in coordinated efforts across the U.S. and U.K., dealing a major blow to one of the most active ransomware gangs. **Evil Corp**, led by Maksim Yakubets, remains sanctioned and linked to Kremlin-based cyber operations. **APT27**, a Chinese state-backed hacking unit, saw multiple indictments involving espionage and financial theft.

Criminal Judicial Actions

Key Insights

94 judicial actions

- October: 27 actions
- November: 25 actions
- December: 42 actions

Financial Impact - Penalties

\$1.31B

Approximately

Indicted

Aleksandr Viktorovich Ryzhenkov

Lockbit: Allegedly used BitPaymer ransomware and hold their sensitive data for ransom.

Sanctioned

16 members of cyber-crime gang Evil Corp

Convicted

Ilya Lichtenstein

Involved in the hack and theft of approximately 120,000 bitcoin from **Bitfinex**.

Sentenced

Mark Sokolovsky - 60 months
Conspiracy to operate
Raccoon Infostealer malware



INTERPOL Arrests 5,500

A global law enforcement operation has led to the arrest of more than 5,500 suspects involved in financial crimes and the seizure of more than \$400 million in virtual assets and government-backed currencies.

Threat Actors

The Q4 2024 data includes 180 tracked threat actor activities from across the globe, representing a broad spectrum of cyber activities including APT (Advanced Persistent Threat) operations, state-sponsored espionage, cybercriminal campaigns, ransomware attacks, and hacktivist movements. While many of these actors appear multiple times due to their involvement in distinct cyber incidents, the overall landscape underscores the prominence of Russia, China, Iran, and North Korea in state-sponsored and APT operations. Eastern Europe and groups of unknown origin account for a significant share of ransomware and cybercriminal activities.

Notably, well-established groups such as **APT29**, **APT38**, **LockBit**, **RansomHub** and **RomCom** continue to play a major role, while a wide array of lesser-known actors also contribute to the evolving and complex global threat environment. This snapshot of Q4 2024 highlights not only the geographic diversity of cyber threats but also the persistent and multifaceted nature of today's threat landscape.

Q4 Active Threat Actors

Cybercriminals

GoldenJackal, BO Team, SideWinder, Water Makara, TA571, Quantum, kzoldyck, IntelBroker, Scattered Spider, TeamTNT, UAC-0218, Waste, Satanic, xenZen, Abyss0, TAG-110, Ghost Tap, Earth Kasha, Water Barghest, LYNX Collective, CyberAv3ngers, TraderTraitor, RiseLoader, MUT-1244, KillSec

State Sponsored Actors

CeranaKeeper, WIRTE APT Group, Islamic Revolutionary Guard Corps, Star Blizzard, Flax Typhoon, Volt Typhoon, Salt Typhoon, Earth Estries, Evasive Panda, Tenacious Pungsan, Liminal Panda, BrazenBamboo, BlueNoroff, TAG-112, Turla, Secret Blizzard, Gamaredon, Venom Spider

APTs

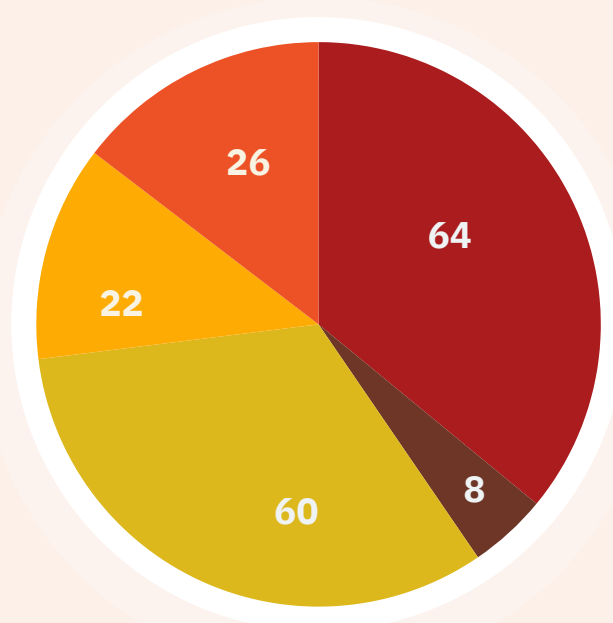
APT29, APT42, APT38, APT31, APT43, APT45, UNC5812, APT-C-35, APT34, TA455, APT37, Louse APT, UNC5820, Evasive Panda, Konni, Earth Estries, Gelsemium, Midnight Blizzard, APT44, RomCom, APT28, WIRTE APT Group, Emennet Pasargad, Handala, APT-K-47, APT-C-60, BrazenBamboo, APT27, APT35, APT41, Bitter, UNC5325, UAC-0125, UAC-0185, APT-C-01, Earth Minotaur

Hacktivists

Nam3L3ss, XakNet, DXPLOIT, NoName057

Ransomware Groups

Fog, Akira, Loki, Black Basta, BianLian, LockBit, Underground, 8Base, BlackCat, Cicada3301, ThreeAm, RansomHub, Rhysida, Embargo, Play, Sarcoma, Nitrogen, Ymir, INC, HellCat, Rhysida, Cactus, FunkSec, ClOp, Termite, Money Message, The ThreeAM, LYNX Collective, BlackSuit, Hunters International, Interlock, Space Bears, Bashe, Abyss, The Money Message, Fog, Brain Cipher



Threat Actors

119

Threat Actors Involved in

180

activities



MOST ACTIVE

Involved in 6 activities each



APT29



RansomHub

Threat Actors

Key Insights, forecast and recommendations

Diverse Targeting Across Sectors and Geographies

Top Targeted Sectors: Government, Financial Services, Technology, Healthcare, Manufacturing, and Critical Infrastructure were consistently targeted.

Global Reach: While North America and Europe were primary targets, attacks were geographically dispersed, affecting organizations worldwide.

State-Sponsored Dominance in Espionage & APTs



Forecast

Continued High Tempo of State-Sponsored Operations:

Geopolitical tensions will continue to fuel espionage and potentially disruptive attacks by actors from Russia, China, Iran, and North Korea. Expect a focus on intelligence gathering related to ongoing conflicts and strategic industries.

Ransomware Evolution and Rebranding:

The ransomware ecosystem will remain dynamic. While some groups may be disrupted (like ALPHV/BlackCat's takedown efforts in late Q4), new groups will emerge, and existing ones may rebrand or splinter. Tactics like double and triple extortion (data encryption, data theft, and DDoS/harassment) will persist.



Russia-linked actors (e.g., APT29)

Highly active (23 recorded campaigns/major activities), focusing on espionage against government, defense, and research sectors adapting TTPs to maintain persistence



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

Maintained high operational activities (25 campaigns/major activities), primarily targeting government, technology, and critical infrastructure



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

With 10 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)

18 campaigns/major activities were heavily involved in financially motivated cybercrime, targeting crypto exchanges and financial institutions to fund state objectives, alongside traditional espionage.

Enhance Threat Intelligence Consumption: Actively monitor threat intelligence feeds for TTPs associated with APT29, APT38, LockBit, RansomHub, RomCom, and actors originating from Russia, China, Iran, North Korea, and Eastern Europe. Focus on intelligence relevant to your specific sector and geography.

Threats

Malware

The landscape of cyber threats is dominated by a variety of ransomware, trojans, spyware, and botnets. Ransomware, such as RansomHub, PlayCrypt, and DragonForce, continues to dominate the threat scene, often leveraging advanced encryption tactics to extort users for financial gain. Meanwhile, Trojans like DCRat, AsyncRAT, and njRAT are frequently deployed to infiltrate systems, exfiltrate data, or serve as backdoors for further malicious activity. The presence of spyware variants like BeaverTail, RedLine, and SpyMax underlines the ongoing risk of data theft, as these tools silently monitor user activity and capture sensitive information.

Botnets, represented by threats like Mirai, Prometei, and Quad7, also highlight the growing trend of distributed denial-of-service (DDoS) attacks and other large-scale disruptions orchestrated by networked malware. Additionally, infostealers and rootkits, such as CloudScout Toolset and PUMAKIT, emphasize the sophistication of modern cyberattacks, targeting valuable personal and organizational data while often evading detection. The combination of these threats presents a multifaceted challenge to cybersecurity professionals.

Top Malware

3 Entries

njRAT

Is a Remote Access Trojan (RAT) commonly used by cybercriminals for gaining unauthorized access to infected systems. Once installed on a victim's machine, njRAT provides attackers with remote control

2 Entries

AsyncRAT

BeaverTail

DCRat

FakeUpdates

FormBook

Killsec

Qilin.B

Remcos

RiseLoader

LightSpy

Helldown

Interlock

Lumma

Stealer

Mirai

Nitrogen

NodeStealer

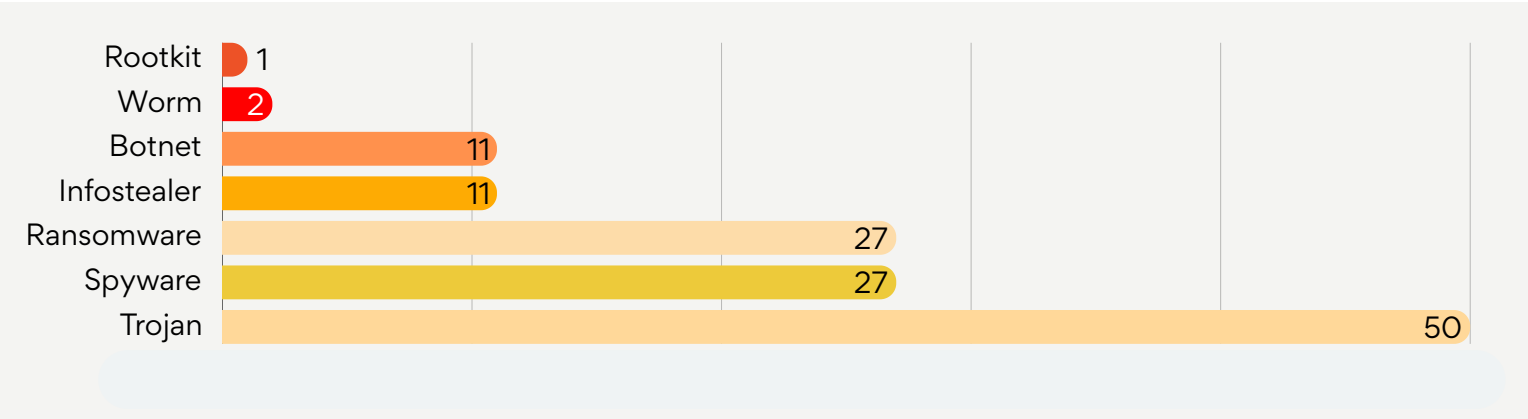
OtterCookie

NEW MALWARE

BianLian

Type: Ransomware

Description: A newly identified strain of ransomware known for its advanced encryption methods and sophisticated evasion tactics. Gained traction in Q4 2024, targeting both personal and corporate networks. Fast-growing and highly evasive, it bypasses traditional security mechanisms, making it a formidable threat.



Threats

Malicious Campaigns



OCTOBER

FakeUpdate' campaign
ClickFix campaign
Prince Ransomware
Midnight Blizzard Spear-Phishing
'I'm not a Robot' reCAPTCHA
Contagious Interview



NOVEMBER

Ymir
Interlock attacks
LastPass Fake Customer Support Number
Election disinformation video
SilkSpecter Fake Online Stores
fake letters Swiss meteorological agency



DECEMBER

Fake Captcha
Session Smart routers
Malvertising Campaign GitHub
Chrome Extension Phishing Attacks
Contagious Interview
Fake LogicalDOC URLs

These ongoing malicious campaigns showcase a wide range of cyberattack methods designed to exploit vulnerabilities across various platforms. The FakeUpdate campaign, for instance, uses compromised websites to trick users into downloading malware disguised as browser or app updates. Similarly, the Contagious Interview campaign, leveraging social engineering tactics, distributes malware under the guise of job interview invitations, often through fake videoconferencing tools or npm packages.

Meanwhile, Prince Ransomware and newer operations like Interlock target specific systems, such as FreeBSD servers, using destructive methods that go beyond traditional data encryption. Fake Captcha and Session Smart Router attacks exploit user trust in familiar security mechanisms to distribute information-stealing malware. Additionally, fraudulent campaigns like LastPass Fake Customer Support Number and SilkSpecter Fake Online Stores rely on impersonating legitimate services to steal sensitive data. These evolving tactics, such as the integration of new malware like OtterCookie, highlight the increasing sophistication of cybercriminals, making it essential for organizations to continuously update their defense strategies.

Threats

Key Insights, forecast and recommendations



Insights

Dominant Threat Categories: Ransomware, Trojans, and Spyware were consistently the most reported malware categories throughout the quarter. This aligns directly with the provided summary highlighting the prevalence of threats like RansomHub, DCRat, and RedLine Stealer.

Forecast

Persistent Ransomware Evolution:

Ransomware will likely remain a leading threat. We can expect attackers to continue refining extortion tactics, potentially increasing the use of multi-extortion techniques (data encryption, data leakage threats, DDoS attacks). Variants like RansomHub, given their Q4 trajectory, may continue to be highly active.

Increased Sophistication and AI Exploitation:

Threat actors may increasingly leverage AI to enhance the effectiveness of phishing campaigns, develop more evasive malware, and create convincing deepfakes for social engineering attacks.

Botnet Diversification:

Botnets will continue to be a tool for DDoS attacks and other large-scale malicious activities. Operators may seek to expand their networks by targeting a wider array of vulnerable devices, including IoT.

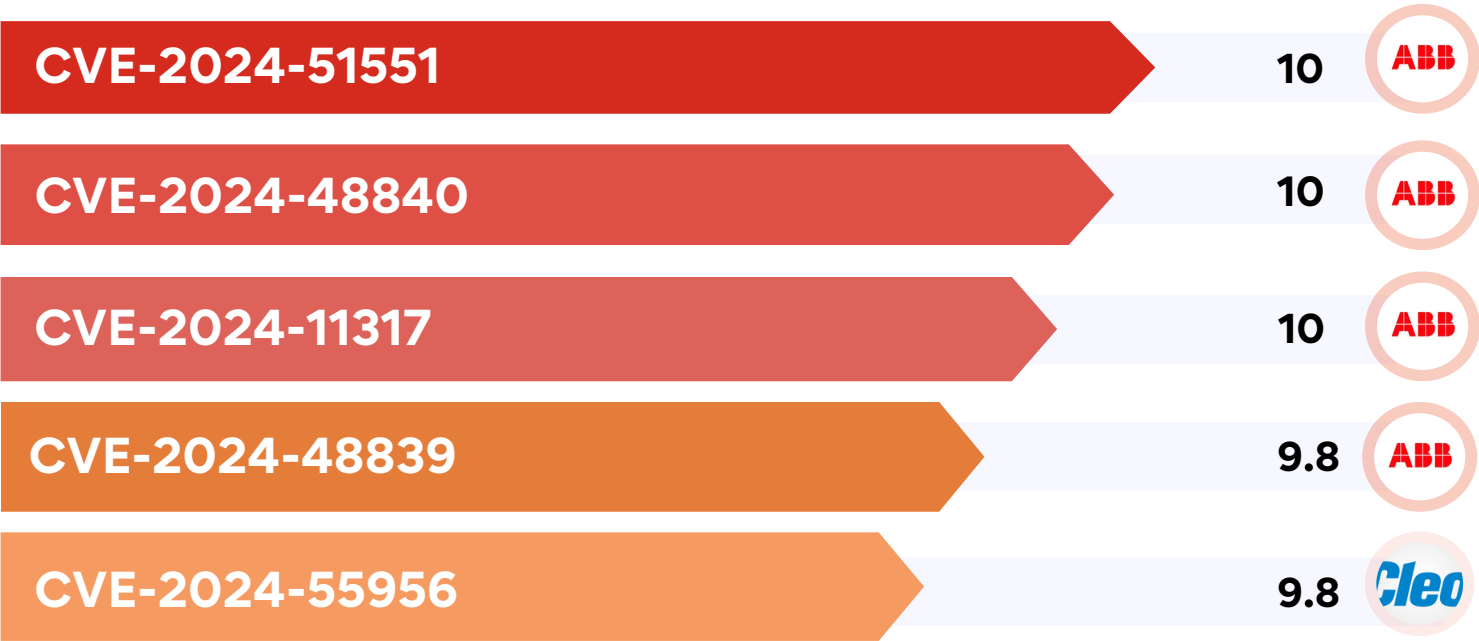
Steadfast Trojan and Spyware Campaigns:

Trojans will remain crucial for initial access, deploying further payloads, and data theft. Spyware will continue to be a major threat due to the high value of compromised credentials and sensitive information.

Top Vulnerabilities

Based on the provided CVE details, a significant concern arises regarding the security posture of ABB's ASPECT Enterprise, NEXUS, and MATRIX Series products. Multiple critical vulnerabilities have been identified, all scoring a perfect or near-perfect CVSS base score of 10 or 9.8. These include the presence of default credentials (CVE-2024-51551), allowing unauthorized access, and several pathways to unauthorized access leading to Remote Code Execution (CVE-2024-48840, CVE-2024-48839) and Session Fixation allowing session takeover (CVE-2024-11317). The concentration of severe vulnerabilities across these ABB product lines suggests a potential systemic issue in their security implementation, posing a high risk of compromise, data breaches, and operational disruption for organizations utilizing these systems.

Beyond the ABB-specific issues, the inclusion of CVE-2024-55956 highlights a separate but equally critical vulnerability affecting Cleo Harmony, VLTrader, and LexiCom. This unauthenticated remote command execution flaw, stemming from default Autorun directory settings and scoring a 9.8, underscores a broader concern about insecure default configurations in widely used software. The potential for attackers to execute arbitrary commands without authentication in these Cleo products presents a severe threat to the integrity and confidentiality of data processed by these systems.



Top Vulnerabilities

Key Insights and recommendations

ICS/OT as a Prime Target:

The significant number of critical vulnerabilities in products from ABB, Rockwell Automation, Johnson Controls, and Delta Electronics, all key players in Industrial Control Systems (ICS) and Operational Technology (OT), is particularly alarming. These systems control physical processes, and their compromise can lead to operational shutdowns, safety incidents, and even physical damage, making them attractive targets for disruptive or destructive attacks.

For stakeholders in the ICS/OT domain

The prevalence of critical vulnerabilities (including Remote Code Execution and default credential issues) in widely used industrial products from vendors like ABB, Rockwell Automation, and Johnson Controls demands immediate and heightened attention. These are not just theoretical IT risks.

The potential for these vulnerabilities to be exploited can lead to significant production downtime, damage to expensive equipment, environmental incidents, and even endanger personnel. Establishing and enforcing strict network segmentation between OT and IT environments, alongside deploying OT-aware monitoring solutions to detect anomalous activity.

1

Insights

Widespread High-Severity Issues Beyond ABB & Cleo

The data reveals numerous other critical vulnerabilities (many CVSS 9.8) affecting major vendors like Rockwell Automation (Remote Code Execution, Path Traversal), Johnson Controls (Missing Authentication), and Delta Electronics (SQL Injection).

2

Insights

Dominance of High-Impact Vulnerability Types:

- Remote Code Execution (RCE) is a prominent threat across several vendors.
- Default Credentials / Missing Authentication offers an easy entry point for attackers.
- SQL Injection continues to be a critical risk for data breaches.

Vulnerable Vendors

The vulnerability landscape is heavily concentrated among a few major vendors, with Microsoft leading at a staggering number of 587 CVEs. This substantial figure underscores the complexity and widespread use of Microsoft products, making them a significant target for cyber threats. Oracle follows at a distant second with 131 CVEs, still a noteworthy number that indicates ongoing security challenges within their enterprise solutions. Linux, a cornerstone of many server infrastructures, presents 125 CVEs, highlighting the persistent need for vigilance in open-source environments. Cisco, with 81 CVEs, and Google, with 73 CVEs, round out the top five, demonstrating that networking equipment and widely used software platforms are also prime targets for exploitation.



Microsoft

587 Vulnerabilities



Oracle

131 Vulnerabilities



Linux (Kernel/Distros)

125 Vulnerabilities



CISCO

81 Vulnerabilities



Google

73 Vulnerabilities

Vulnerable Vendors

Key Insights and recommendations

ICS/OT as a Prime Target:

The significant number of critical vulnerabilities in products from ABB, Rockwell Automation, Johnson Controls, and Delta Electronics, all key players in Industrial Control Systems (ICS) and Operational Technology (OT), is particularly alarming. These systems control physical processes, and their compromise can lead to operational shutdowns, safety incidents, and even physical damage, making them attractive targets for disruptive or destructive attacks.

For stakeholders in the ICS/OT domain

The prevalence of critical vulnerabilities (including Remote Code Execution and default credential issues) in widely used industrial products from vendors like ABB, Rockwell Automation, and Johnson Controls demands immediate and heightened attention. These are not just theoretical IT risks.

The potential for these vulnerabilities to be exploited can lead to significant production downtime, damage to expensive equipment, environmental incidents, and even endanger personnel. Establishing and enforcing strict network segmentation between OT and IT environments, alongside deploying OT-aware monitoring solutions to detect anomalous activity.

1

Insights

Widespread High-Severity Issues Beyond ABB & Cleo

The data reveals numerous other critical vulnerabilities (many CVSS 9.8) affecting major vendors like Rockwell Automation (Remote Code Execution, Path Traversal), Johnson Controls (Missing Authentication), and Delta Electronics (SQL Injection).

2

Insights

Dominance of High-Impact Vulnerability Types:

- Remote Code Execution (RCE) is a prominent threat across several vendors.
- Default Credentials / Missing Authentication offers an easy entry point for attackers.
- SQL Injection continues to be a critical risk for data breaches.

Incidents Impact

The top five incidents in terms of the number of people affected reveal a substantial impact, with figures reaching from tens of millions to nearly 200 million individuals. The incident with the largest number of affected persons is a ransomware attack on Change Healthcare, estimated to have impacted 190,000,000 people. Following this, a data breach associated with DemandScience affected 122,000,000 people. Other significant incidents include a data breach at Hot Topic impacting 57,000,000 records, an incident involving Comcast Cable Communications LLC affecting 35,000,000 customers, and a cyberattack on Star Health Insurance affecting 31,000,000 people.

The occurrence of these large-scale incidents across diverse industries suggests that no sector is immune to the risk of breaches affecting a significant portion of the population. Further examination could explore the types of data compromised, the nature of the attacks, and their geographical distribution to gain deeper insights into the evolving threat landscape.


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



190M  

122M  

57M  


COMCAST
35M
CUSTOMERS


STAR Health Insurance
The Health Insurance Specialist
31M
PATIENTS


PIH HEALTH
17M
RECORDS

Incidents Impact

Key Insights

Top 5 breaches

The quarter was dominated by a small number of catastrophic incidents that affected hundreds of millions of individuals. The top five breaches alone impacted over **435 million people**, demonstrating that the primary threat is not the frequency of attacks, but the astronomical impact of a single, successful intrusion into a data-rich environment.

Ransomware as the primary weapon

Ransomware, in particular, proved its potential for mass disruption with the Change Healthcare attack, which affected not just data privacy but critical real-world services.

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.

No Sector is Immune, But Some Are Prime Targets:

Incidents were recorded across a wide range of industries, including finance, retail, government, and manufacturing, proving that every organization is a potential target. However, sectors holding vast and sensitive datasets, Healthcare, Technology, Telecommunications, and large-scale Retail, were disproportionately impacted and are clearly in attackers' crosshairs.

Affected Industries

Analyzing the incident data reveals that the top 5 most affected sectors include Government (81 incidents), Healthcare (75 incidents), Education & Research (38 incidents), Consumer Products & Retail (37 incidents), Financial Services (34 incidents). These sectors represent the areas with the highest frequency of reported incidents within the dataset.

Examining the impact on individuals within these top sectors shows significant variation in the amount of people affected. Healthcare, despite having slightly fewer incidents than Government, reported a substantially higher number of people affected, exceeding 225 million. Consumer Products & Retail also shows a high number of affected individuals at over 63 million.



Financial Services

34



**Consumer
Products & Retail**

37



Education

38



Healthcare

75



Government

81

Affected Industries

Key Insights

Key Insights by Sector

The Q4 2024 data shows that while cyber risk is universal, the impact is highly concentrated in sectors that serve as custodians for massive volumes of sensitive personal and health information. Attackers are strategically targeting these industries to maximize the value and impact of a single breach.

Healthcare:

Ground Zero for Impact

The Healthcare sector was, by an enormous margin, the most impacted industry during Q4, primarily due to the single, colossal ransomware attack on Change Healthcare (190 million individuals affected). This incident underscores the sector's position as a top-tier target due to the immense value of Personal Health Information (PHI). The attack highlighted a critical vulnerability where the disruption of one central entity can paralyze administrative and care-delivery functions across the entire industry.

- Total Affected: **Over 191 million**
- Key Incident: **Change Healthcare**

Technology & Business Services:

The Risk of Big Data

This sector, exemplified by the DemandScience breach (**122 million affected**), faces extreme risk due to its business model. Companies that collect and manage data are treasure troves for attackers. A breach here not only compromises personal data but can also trigger a catastrophic supply-chain crisis for their customers.

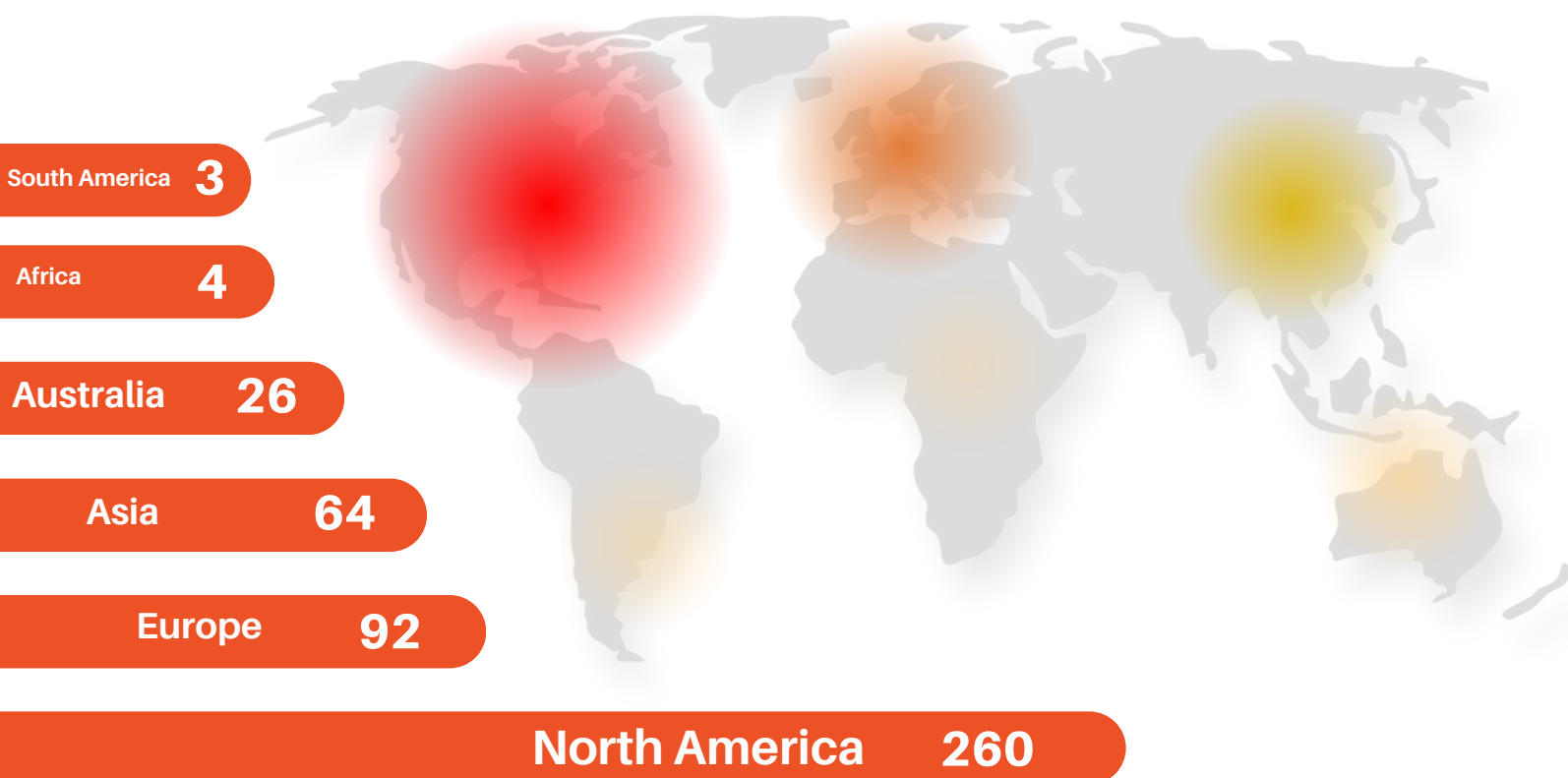


Government:

The Most Frequent Target

Even though it did not suffer an incident on the scale of those in the healthcare sector, the Government sector recorded the highest number of individual security incidents in Q4. This indicates a persistent, widespread campaign by threat actors against government entities at local, state, and national levels. While these attacks were individually smaller, 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



Insight

Out of the 478 entries analyzed, 29 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 245 incidents, followed by Japan with 29, Australia with 23, France with 18, 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 breached in Q4 2024 reveals a significant concentration of high-impact incidents in North America, particularly the United States. However, the presence of a major breach in India underscores the global nature of cyber risk.



United States as the Epicenter of Mega-Breaches

- The overwhelming majority of individuals affected during Q4 were impacted by breaches at U.S.-based companies. Four of the five largest incidents (Change Healthcare, DemandScience, Hot Topic, and Comcast) are headquartered in the USA.
- In total, incidents reported by U.S. companies in this dataset accounted for over 404 million affected individuals, representing approximately 91% of the total for the quarter.



Significant Impact in Asia

- The cyberattack on India-based Star Health Insurance was one of the top five global incidents, affecting **31 million people**. This highlights that significant cyber threats are a major concern outside of North America and can impact populations on a massive scale.
- The full dataset shows incidents occurring across the globe, including in the United Kingdom, Australia, and other parts of Europe and Asia.

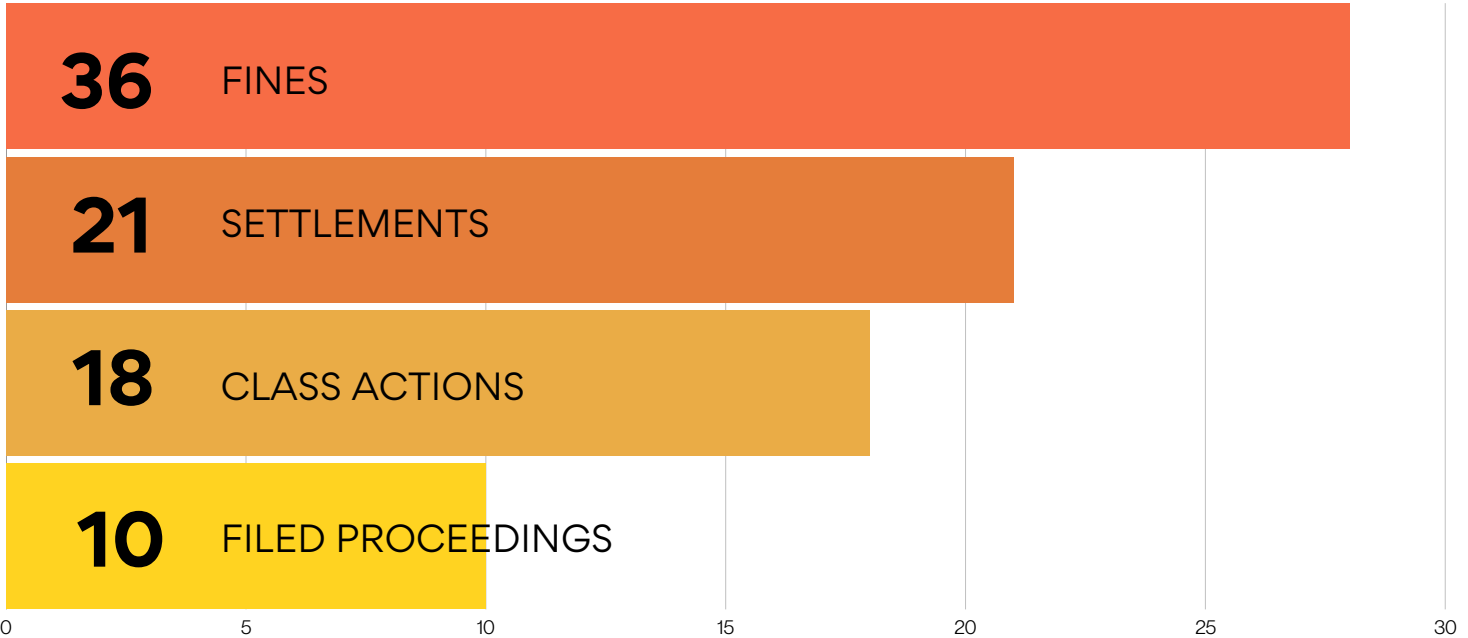
Recommendations

- **Implement a Geo-Specific Risk Strategy:** Your cybersecurity strategy cannot be one-size-fits-all. It must account for the different regulatory environments (e.g., GDPR in Europe, PIPEDA in Canada, etc.), threat actors, and geopolitical risks specific to each region of operation.
- **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.
- **Centralize Threat Intelligence:** Use a centralized model to gather and analyze threat intelligence from all operational regions. An attack method seen in one country today is likely to be deployed in another tomorrow. A global view is essential for proactive defense.

Civil Judicial Actions

In Q4 2024, the financial impact of legal actions was substantial, with significant monetary penalties and settlements recorded across the quarter. October saw the highest single penalty amount at \$310 million, associated with a 'Fine,' and the month's total penalties reached \$394.58 million. November's highest penalty was \$115 million, linked to a 'Class Action,' and the total for the month was \$157.79 million.

December had the second-highest single penalty at \$280 million, again for a 'Fine,' with a total of \$361.61 million in penalties. Overall, the total monetary impact of legal actions in Q4 2024 amounted to approximately \$913.97 million, highlighting the significant financial consequences of the legal proceedings during this period. The data indicates that while individual fines can be very high, class action settlements also contribute substantially to the overall financial landscape of legal outcomes.





META
\$280,577,026 - FINE



Marriott International, Inc
\$52,000,000 - FINE

Civil Judicial Actions

Key Insights and recommendations

Consumer Protection is the Primary Legal Ground:

The most cited legal basis for action was "Consumer Protection," highlighting a strong regulatory focus on safeguarding consumer rights and interests. "Regulatory Compliance" and "Data Privacy" followed, indicating a multi-faceted approach to corporate oversight.



Fines are the Most Common Outcome:

'Fine' is by far the legal action type with the highest total penalty amount, reaching over \$669 million. This indicates that when a fine is imposed, it tends to be substantial.



Class Actions and Settlements are Significant

'Class Action' and 'Settlement' also contribute significantly to the total penalty amounts, with over \$143 million and \$101 million respectively. While their average penalties are lower than 'Fines', they still represent substantial financial consequences.

Conclusion

The findings in this Q4 2024 report reflect a rapidly evolving threat landscape marked by increased malware development, active ransomware groups, and a high volume of disclosed vulnerabilities. The continued activity of both opportunistic and targeted threat actors reinforces the importance of proactive defense strategies, real-time threat intelligence, and coordinated response efforts.

Organizations must remain vigilant, adapt their security postures, and invest in technologies and training to mitigate the growing complexity of cyber threats. As we move into the next quarter, maintaining resilience through collaboration, threat sharing, and strategic planning will be essential for staying ahead of adversaries.

Methodology

This **Hall of Hacks** report provides a comprehensive overview of the Q4 2024 cybersecurity landscape 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 landscape, 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 Q4 2024 cybersecurity landscape.

Sources:





Prepared by:

Sofia V.

Marc R.

Nicolas P.

✉ hello@cybermaterial.com

🌐 cybermaterial.com/hall-of-hacks



Powered by



<https://911cyber.app>

Copyright 2025 © CyberMaterial.

No part of this document may be distributed, reproduced or posted without the express written permission of CyberMaterial.



Hall of Hacks

Copyright 2025 © CyberMaterial.

No part of this document may be distributed, reproduced or posted without
the express written permission of CyberMaterial.