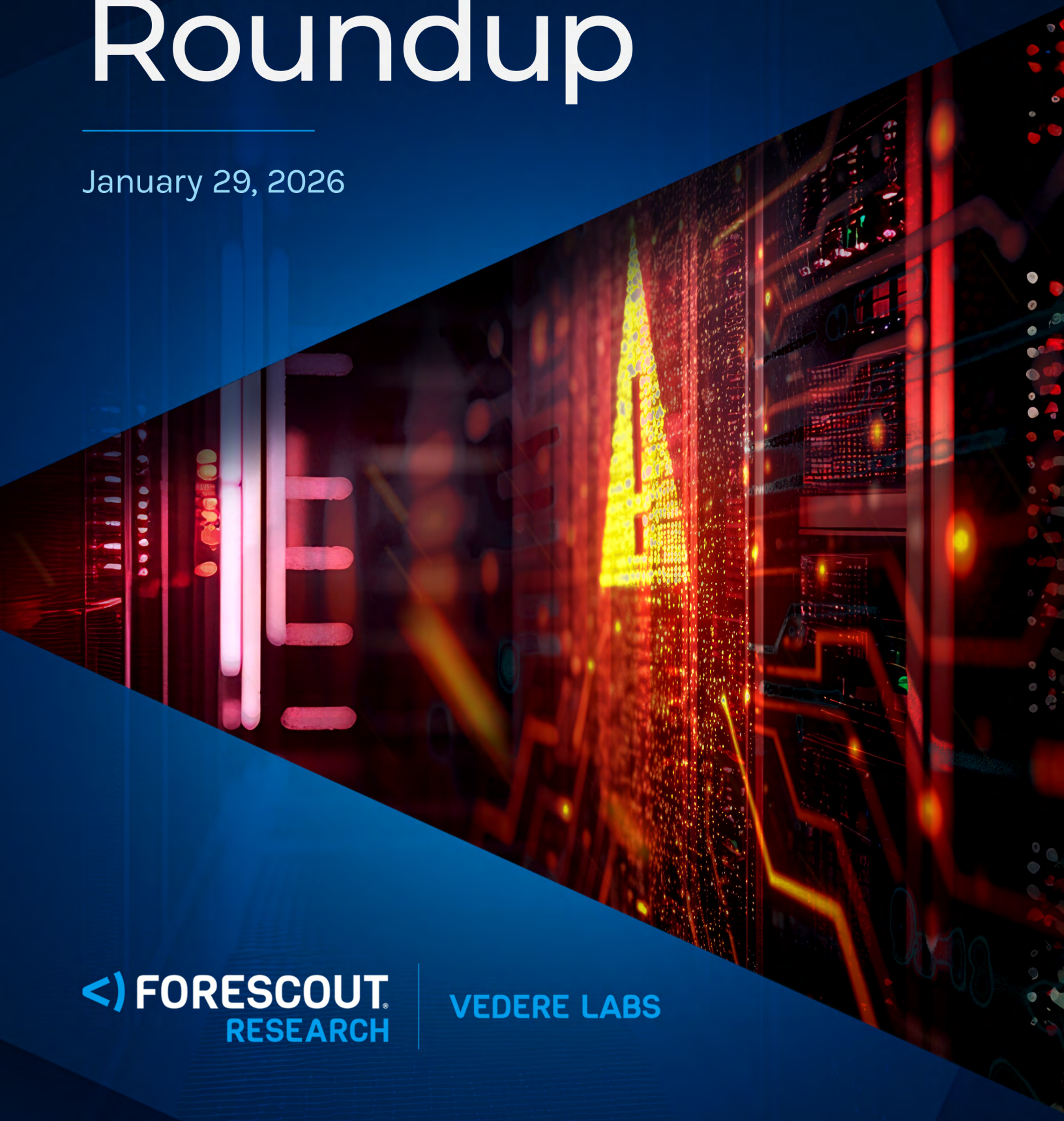
2025 Threat Roundup

January 29, 2026



FORESCOUT RESEARCH | VEDERE LABS

Contents

1. Executive Summary 3

2. Main Findings 6

2.1. Location – Attacks Become More Distributed 6

2.2. Autonomous Systems – Mixing Compromised And Benign Infrastructure 7

2.3. Attacked Services – Vulnerabilities Over Credentials 8

2.4. Weak Credentials – Focusing on Databases 10

2.5. Exploits – The Rise of Network Infrastructure 11

2.6. OT Attacks – Modbus is the Undisputed Leader 13

2.7. Attacker Actions/TTPs – Discovery Continues To Dominate 14

2.8. Malware – Everything Remains as It Never Was 15

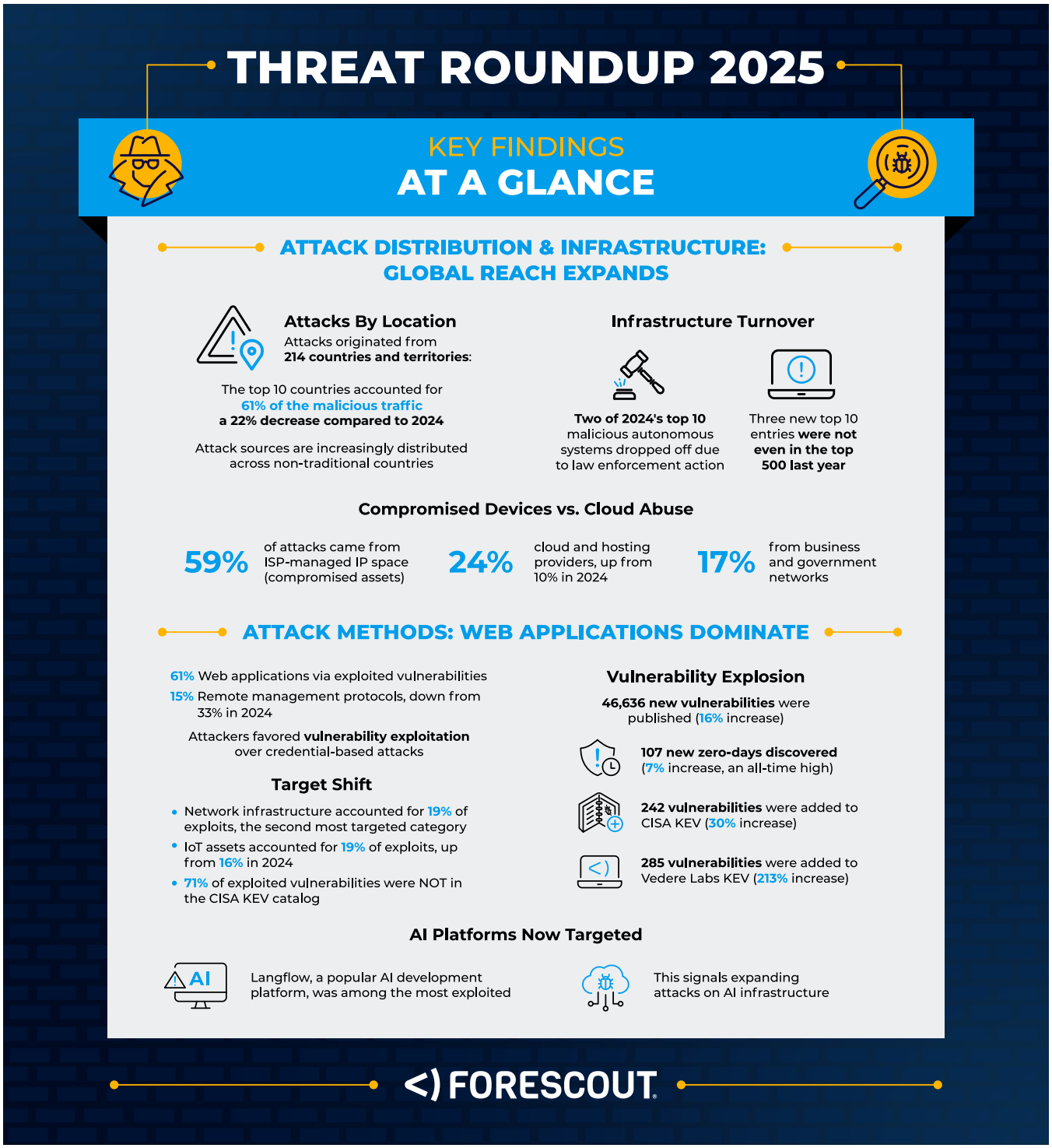
2.9. Threat actors – Focus on Critical Infrastructure 17

2.10 Incidents and Data Breaches – Cybercrime is Widespread 22

3. Mitigation Recommendations 24

1. Executive Summary

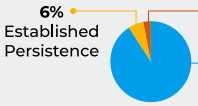
Each year, Forescout Research – Vedere Labs analyzes the evolving threat landscape by reviewing the attack telemetry and threat actor intelligence we collect. The rising volume, sophistication, and costs of cyberattacks will keep cybersecurity a board-level priority in 2026. This report analyzes 2025 data and provides tactical insights and strategic recommendations to strengthen defenses in 2026.



THREAT ROUNDUP 2025

KEY FINDINGS AT A GLANCE

POST-BREACH BEHAVIOR: ATTACKERS SPEND MORE TIME EXPLORING



OT Attacks Surged 84%

57% Modbus 22% Ethernet/IP 8% BACnet

Malware Trends

Remote access trojans (RATs) and infostealers were tied at 35% each

Botnets accounted for 12% down from 29% in 2024

THREAT ACTORS & INCIDENTS

Geographic Concentration

178 countries were targeted:

1. 276 United States
2. 154 India
3. 149 Germany

Threat Actor Origins

1. 210 China
2. 112 Russia
3. 55 Iran

Industry Targets

Most Targeted:

Financial Services

Government

Telecommunications

Fastest Growth: 16% Manufacturing 13% Healthcare

Incident Reality Check

We analyzed **1189 incidents** across 95 countries

Cybercriminals were responsible for **6x more incidents than** state-sponsored actors

Although **China** hosts more **threat actors**, **Russia** came ahead in **number of incidents**

HEALTHCARE CRISIS: DATA BREACH EPIDEMIC

600+ healthcare data breaches in the US

Average impact: 71,996 individuals per breach

1M **Eight breaches** each affected more than 1 million people

80% of these breaches were attributed to hacking incidents

FORESCOUT

Where Does Our Data Come From?

Most of the data in this report comes from the Vedere Labs Adversary Engagement Environment (AEE): a set of internet-exposed honeypots designed to lure attackers and record their interactions. In the AEE, "*attacks*" represent a range of malicious actions, including port scanning and brute forcing. Between January and December 2025, the AEE recorded more than 900 million attacks. A subset of these includes **exploit** attempts against known vulnerabilities with a specific CVE identifier.

This dataset differs from many threat reports because it comes from specialized IT, OT, IoT, and IoMT honeypots that either mimic realistic asset profiles – including exposed protocols, banners and parts of the file system – or **are *real*** specialized assets, rather than generic honeypots capturing broad non-specific activity.

Our Malware Analysis Lab (MAL) collects and analyzes malware samples dropped on the AEE or shared in public repositories. The goal is not volume, but uniqueness; to focus on samples that are distinct and representative. **Between January and December 2025, MAL analyzed thousands of unique malware samples.**

Finally, Vedere Labs continuously hunts for new command-and-control (C2) infrastructure and maintains a threat actor knowledgebase with **data on nearly 900 threat actors**.



2. Main Findings

2.1. Location – Attacks Become More Distributed

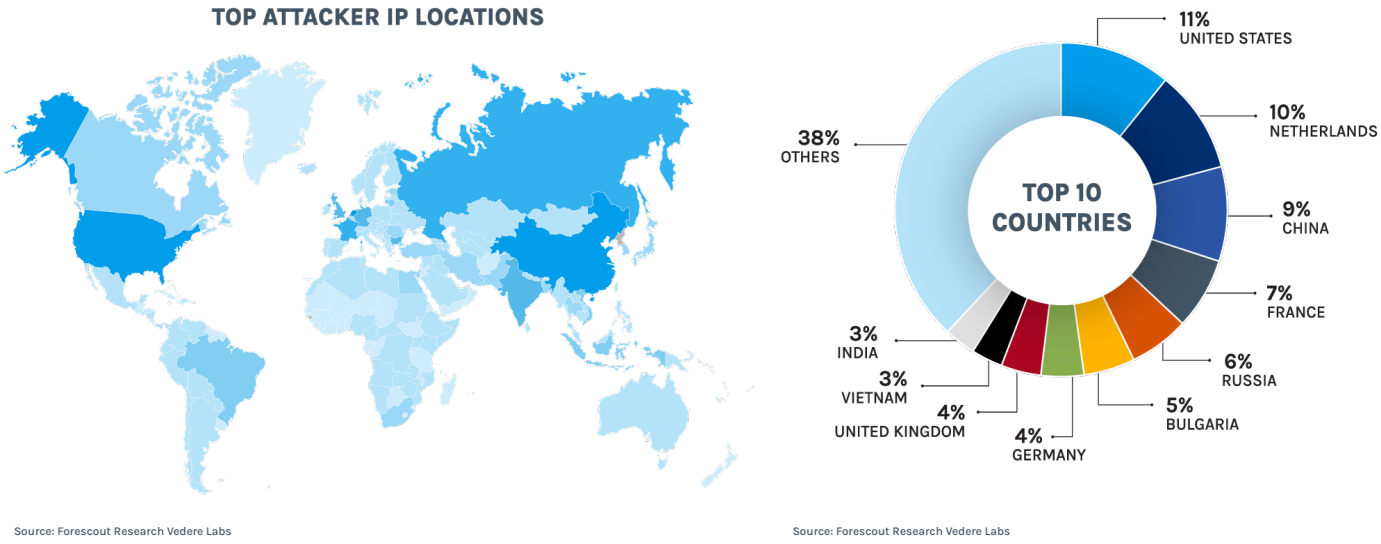


Figure 1 – Distribution of attacks by IP address country of origin

Figure 1 shows the distribution of attacks by country of origin. We observed attacks originating from 214 countries and territories. Countries appear in this dataset for several reasons: legitimate hosting providers are abused by attackers; bulletproof hosting providers explicitly support criminal activity; or compromised hosts are used to launch attacks.

In 2025, the top 10 countries accounted for 61% of malicious traffic - a 22% decrease compared to 2024 - and a reversal of a trend observed since 2022, when that figure was 73%. In other words, **attacks are more distributed and attackers are using IP addresses from less common countries more frequently**. This may reflect a combination of more compromised assets and greater use of leased infrastructure in those regions.

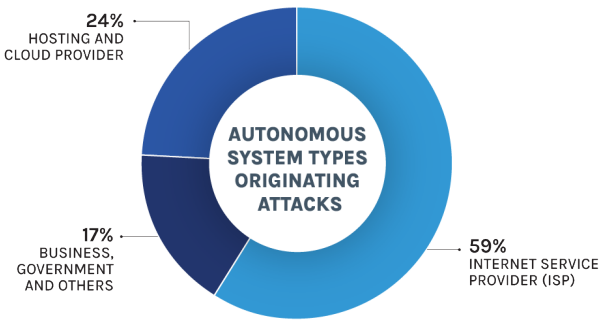
The top 10 countries list changed in two places compared with 2024: France and India replaced Poland and Estonia. Rankings also shifted materially. **Russia decreased from 16% to 6% of attacks, while China increased from 8% to 9%.** The United States accounted for 11% and the Netherlands accounted for 10% of the attacks.

Country of origin is not direct attribution of where attackers are located, it reflects where traffic appeared to originate when it reached our honeypots. As discussed in section 2.2, threat actors continue to use techniques designed to obscure their true location, and as shown in section 2.9, our threat actor database indicates that most actor groups are associated with China (although that does not imply that most individual attacks originate there).

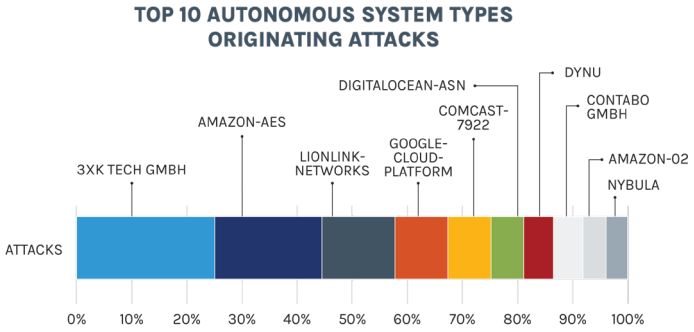


Insight for defenders: Country of origin alone remains an unreliable indicator of IP risk. However, the continued presence of Russian and Chinese IP ranges among the top sources reinforces guidance from previous years: if your organization does not operate in, or conduct business with, those countries, blocking those ranges can reduce noise in the SOC.

2.2. Autonomous Systems – Mixing Compromised And Benign Infrastructure



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

Figure 2 – Distribution of attacks by originating Autonomous System

Attacks originated from more than 500 autonomous systems (ASes) which are blocks of IP addresses controlled by an organization. Figure 2 shows the percentage of attacks associated with three AS categories:

- **Internet Service Providers (ISPs)**: 59% in 2025, up from 57% in 2024.
- **Business, government, and other networks**: 17% in 2025, down from 33% in 2024.
- **Hosting or cloud providers**: 24% in 2025, up from 10% in 2024.

The large share of attacks originating from ISP-managed space suggests that **attackers continue to favor compromised assets over leased infrastructure from dedicated providers**. This is consistent with 2024. However, we did not observe a new distinct routing technique this year. We highlighted residential proxies in 2023 and Operational Relay Boxes (ORBs) in 2024.

What did change was the **increased abuse of benign infrastructure for malicious activity, particularly cloud services**. Examples include the use of Telegram and frontend hosting providers in phishing campaigns as well as Discord for malware command and control. The “hosting and cloud providers” category grew for the first time since 2023, more than doubling from 10% to 24%. Abuse of Amazon and Google infrastructure remained significant accounting for more than 15% of attacks, up from 11% in 2024. Within that category, AMAZON-02 jumped from 16th in 2024 to ninth in 2025. Alibaba, a major China-based cloud provider, jumped from sixth in 2024 to 13th in 2025.

Overall, the top 10 ASes accounted for 45% of attacks, down 3 percentage points from 2024 - another indicator of increasing distribution. Five ASes from the 2024 top 10 remained in the top 10 in 2025: AMAZON-AES, LIONLINK-NETWORKS, GOOGLE-CLOUD-PLATFORMS, DIGITALOCEAN-ASN, and Contabo GmbH.

Notable absences from the 2025 top 10 include:

- **Xhost Internet Solutions LP**: The top AS in our 2024 report was sanctioned by the United States, Australia, and the United Kingdom for connections to hosting provider Zservers, which provided services to the LockBit ransomware gang and other cybercriminal groups. Activity did not disappear, however: this AS ranked 17th in our 2025 dataset.
- **Proton66 OOO**: The fourth most common AS in 2024 ranked 22nd in 2025. Proton66 was linked to bulletproof hosting providers SecureHost and BEARHOST in late 2024. These providers were advertised

on underground platforms and used for phishing, malware distribution, and spam. There was no law enforcement action against these providers in 2025, but attackers may have shifted to other providers to reduce exposure.

Notable new ASes in the 2025 top 10 include:

- **3xK Tech GmbH**: The top AS of 2025 is based in Germany. It has not been publicly linked to a bulletproof hosting provider, but it appeared in several campaigns throughout the year, most notably login attempts against VPN portals.
- **Dynu Systems Incorporated**: The seventh-ranked AS is based in the United States and is primarily a dynamic DNS provider. Some malicious domains have been associated with the service, but there is no connection to any known bulletproof hosting provider.
- **Nybula LLC**: The tenth-ranked AS is a known bulletproof hosting provider registered in the United States and was frequently used by Russian threat actors in 2025. On November 12, hundreds of servers were seized by Dutch police in connection with this provider.

None of these ASes were in the top 500 observed in 2024, indicating rapid turnover at the top of the infrastructure stack. Organizations should monitor this shifting landscape to understand which networks are most likely to generate hostile traffic.



Insight for Defenders: Autonomous System context remains a stronger risk signal than country of origin. IPs associated with historically risky ASes should be handled cautiously, especially those that persist in the top 10 and are not primarily mainstream cloud services. The continued use of compromised assets to route attacks also reinforces the need for timely threat intelligence on compromised infrastructure and the asset types most frequently abused.

2.3. Attacked Services – Vulnerabilities Over Credentials

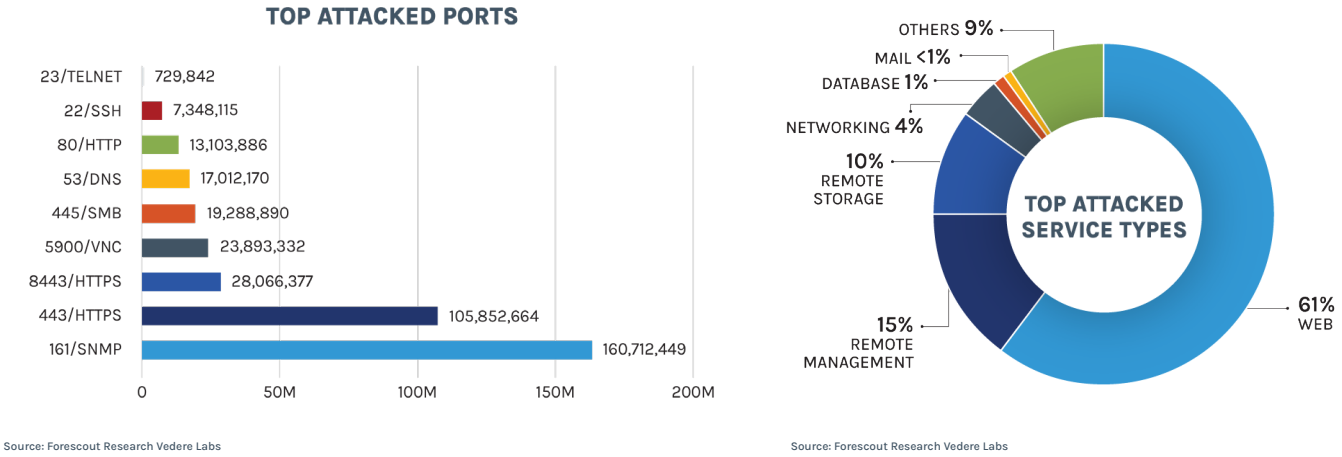


Figure 3 – Distribution of attacked ports and services

Figure 3 shows the share of attack traffic targeting each type of network service, classified by assigned or well-known IPv4 TCP destination ports.

Notable Increases

- **Web applications: 61% in 2025**, up from 41% in 2024, a 20 percentage point increase.
  - Primary attack method: vulnerability exploitation and scanning.
  - Now the dominant target by a wide margin.
- **Networking protocols**: 4% in 2025, up from 3% in 2024.
  - Includes DNS, DHCP, and CWMP/TR-069.

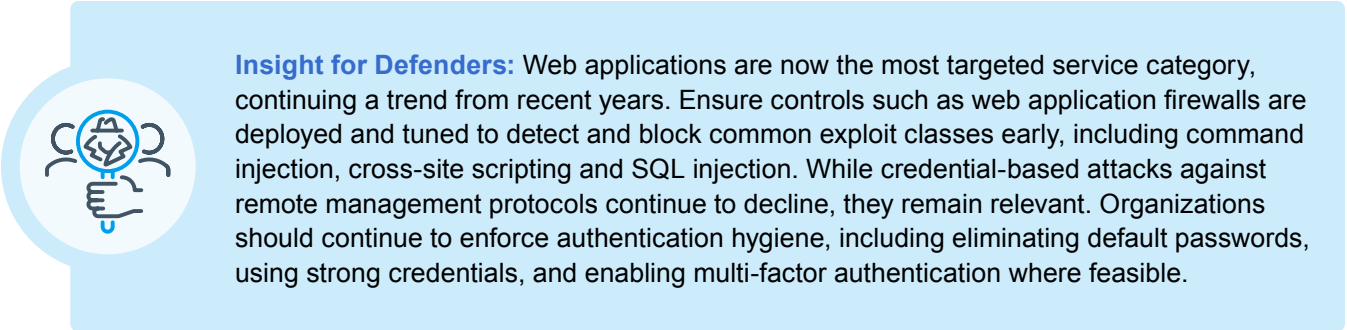
Sharp Declines

- **Remote management: 15% in 2025**, down from 33% in 2024, and down from 43% in 2022.
  - Includes RDP, VNC, SSH, and Telnet.
  - Primary attack method: brute forcing and password spraying.
- **Remote storage**: 10% in 2025, down from 19% in 2024.
  - Includes SMB and FTP.
  - Continuing a three-year decline, 23% in 2022, 20% in 2023, 19% in 2024, and 10% in 2025.
  - Primary attack method: Brute forcing.

Stable Targets

- **Database services: 1% in 2025**, unchanged from 2024.
  - Microsoft SQL Server, Redis, MongoDB, MySQL, PostgreSQL.
- **Email services: <1% in 2025**, unchanged since 2022.
  - IMAP, POP3, SMTP.

These findings reinforce a trend we have tracked since 2022: attackers increasingly favor vulnerability exploitation over credential-based attacks for initial access.



Insight for Defenders: Web applications are now the most targeted service category, continuing a trend from recent years. Ensure controls such as web application firewalls are deployed and tuned to detect and block common exploit classes early, including command injection, cross-site scripting and SQL injection. While credential-based attacks against remote management protocols continue to decline, they remain relevant. Organizations should continue to enforce authentication hygiene, including eliminating default passwords, using strong credentials, and enabling multi-factor authentication where feasible.

2.4. Weak Credentials – Focusing on Databases

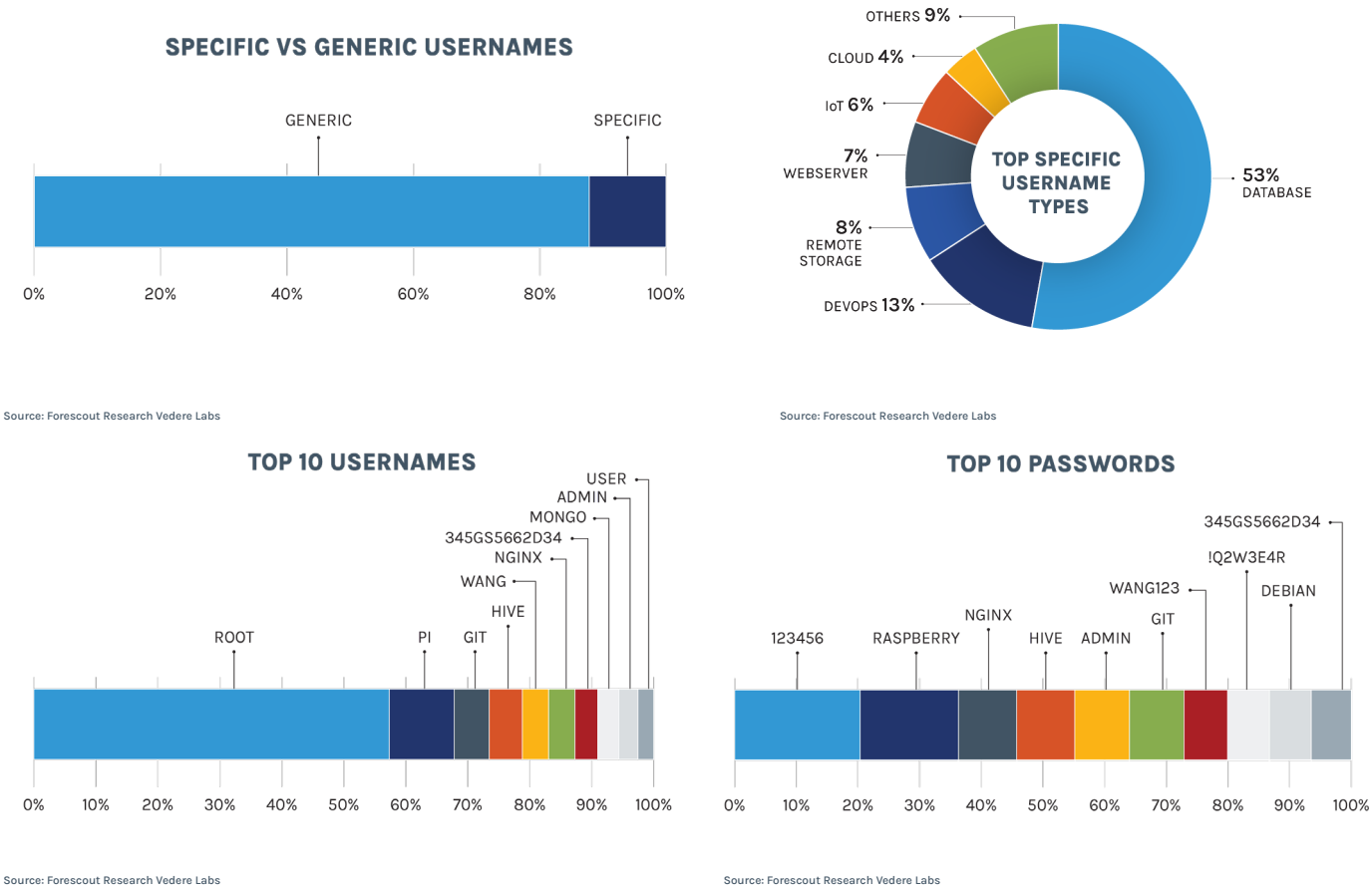


Figure 4 – Top abused credentials

Figure 4 shows the most abused credentials we observed, divided into two categories: generic and specific usernames.

Generic usernames include “root,” “admin,” “user,” “guest,” and similar accounts. The decrease from 95% in 2024 to 88% in 2025 suggests that attackers are placing more emphasis on targeting specific assets and applications, rather than relying solely on brute forcing and dictionary attacks. We also observed an “internationalization” trend in generic usernames. For example, we saw the financial term “accounts” used in multiple languages, including “comptes” (French), “cuentas” (Spanish) and “hesaplar” (Turkish), likely reflecting targeting of small and medium-sized businesses across different geographies.

Specific usernames increased from 5% in 2024 to 12% in 2025 and can be associated with roles, such as “www,” “backup,” and “deployer,” as well as specific applications and platforms, such as “odoo,” “rpi,” “kafka,” “zabbix” or “ec2-user”. Given the overall increase in specific usernames, it’s important to examine which types of specific credentials attackers most frequently abused:

- **Databases**: 53% in 2025, down from 64% in 2024. Top database usernames included “hive”, “mongo”, “oracle”, “gpadmin” and “mysql”.
- **DevOps**: 13% in 2025, up from 9% in 2024. Top usernames included “git”, “developer”, “gitlab”, “lighthouse” and “flask”.
- **IoT**: continued to decline. It was the most common category in 2023, fourth in 2024, and fifth in 2025. This likely reflects attackers’ preference for vulnerability exploitation against IoT assets, rather than reduced

interest in those targets. Common usernames included “pi” (Raspberry Pi), “ubnt” (Ubiquiti routers), “moxa” (industrial networking) and “zyfwp” (Zyxel firewalls).

Insight for Defenders: Strong credential management remains essential for reducing exposure to attacks that leverage weak or default credentials. For practical guidance, NIST’s updated version of its digital identity guidelines are worth reviewing, particularly where they challenge long-held assumptions about password complexity and periodic password changes.

2.5. Exploits: The Rise of Network Infrastructure

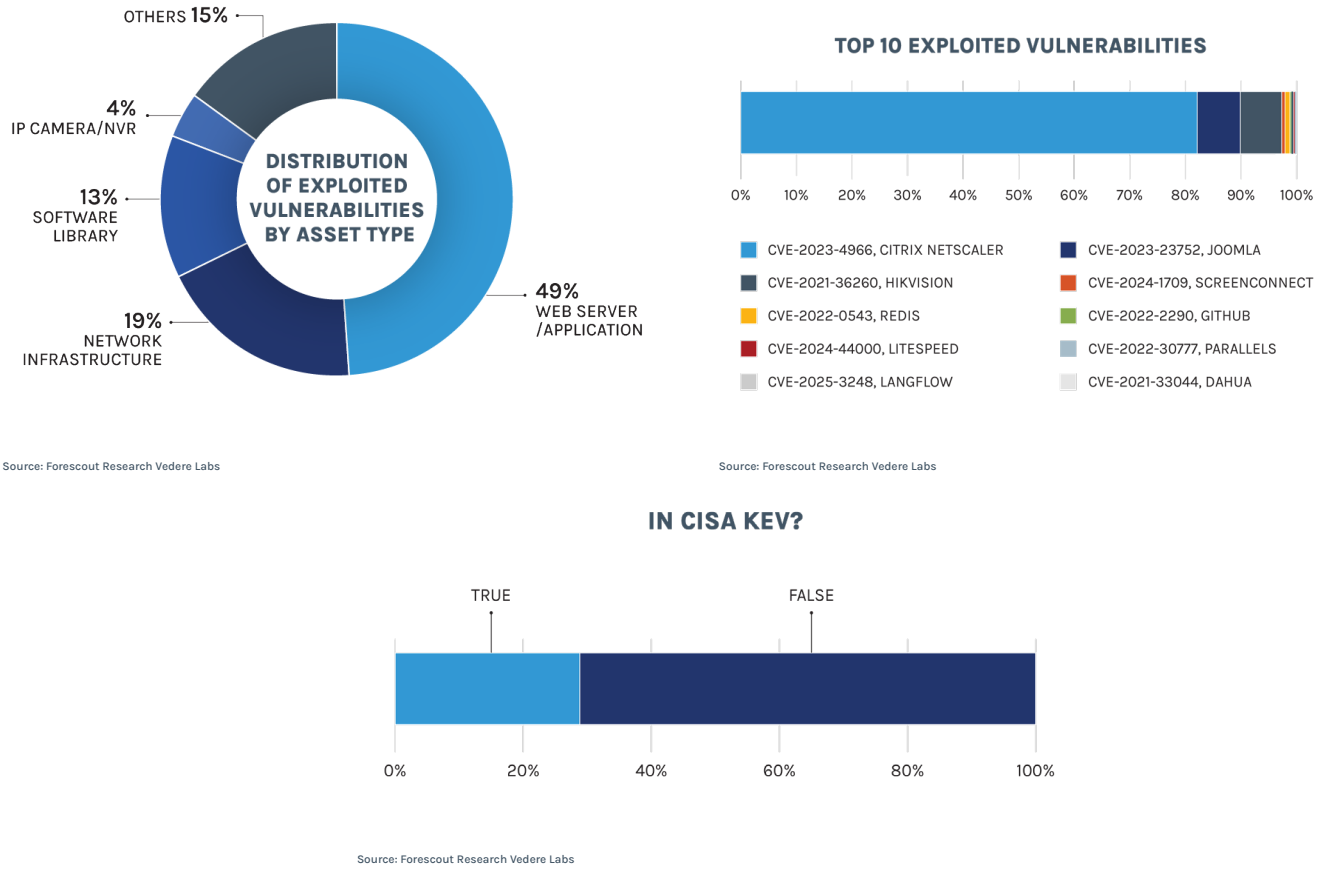


Figure 5 – Vulnerabilities exploited during the study period

As of December 18, 2025, there were 46,636 newly published vulnerabilities, up 16% from 40,303 in 2024. We also tracked 107 new zero-days, up 7% from 100 in 2024, 242 vulnerabilities added to CISA’s KEV catalog, up 30% from 186 in 2024, and 285 vulnerabilities added to the Vedere Labs KEV list, up 213% from 91 in 2024.

Figure 5 shows the distribution of vulnerabilities targeted for exploitation:

Still dominant, but declining

- **Web servers and applications: 49% in 2025**, down from 56% in 2024.
  - First decrease after three years of growth, 14% in 2022, 36% in 2023, and 56% in 2024.
  - Remains the largest exploit category.

Rapid Growth Categories

- **Network infrastructure: 19% in 2025**, up from 14% in 2024.
  - Includes firewalls, routers, and VPN appliances.
  - Four-year surge: 3% in 2022, 11% in 2023, 14% in 2024, and 19% in 2025.
  - Now the second most exploited category.
  - We discussed this trend in our 2025H1 threat review and expect it to remain elevated in 2026.

- **IoT assets: 19% in 2025**, up from 16% in 2024.
  - IP cameras and NVRs accounted for 4% of all exploits.
  - Tied with network infrastructure as the second-largest category.

Sharp Decline

- **Software libraries**: 13% in 2025, down from 14% in 2024.
  - Three-year decline, 76% in 2022, 29% in 2023, 14% in 2024, and 13% in 2025.

Additional observations:

- **Five of the top 10 most exploited vulnerabilities from 2024 remained in the top 10 in 2025**:
  - **CVE-2023-4966 (Citrix NetScaler)**: appeared as a zero-day in 2023, was the most exploited in 2024, and remained in that position in 2025.
  - **CVE-2023-23752 (Joomla)**: moved from sixth most exploited in 2024 to second in 2025.
  - **CVE-2021-36260 (Hikvision)**: remained third most exploited in both 2024 and 2025.
  - **CVE-2024-1709 (ScreenConnect)**: moved from seventh in 2024 to fourth in 2025.
  - **CVE-2022-0543 (Redis)**: the only vulnerability on this list since 2022, and it remained fifth in both 2024 and 2025.
- **A new entry highlights emerging exploitation of AI infrastructure: CVE-2025-3248 (Langflow)** was the only 2025 vulnerability in the top 10. It affects a platform used to build AI-powered agents and workflows. **As AI adoption expands, related platforms and components are likely to become attractive targets for exploitation.**
- **Most exploited vulnerabilities still fall outside CISA KEV**: The share of exploited vulnerabilities not in the CISA KEV catalog remained high at 71%, down 2 percentage points from 2024. While we did not update last year's dedicated analysis of this gap, growth in alternative KEV catalogs suggests the industry is responding as attackers probe more of organizations' attack surface beyond traditional endpoints.
- **Additional OT vulnerabilities exploited outside CISA KEV**: Last year's report listed 25 CVEs in OT assets that were exploited, based on AEE data or observations from the Shadowserver Foundation, but were not included in CISA KEV. This year, the list includes six additional entries:
  - **CVE-2023-5222 (Viessmann Vitogate 300)**: a gateway used to connect LON and BACnet or Modbus networks.
  - **CVE-2024-11305 (APsystems Altenergy)**: used for solar inverter monitoring and control.
  - **CVE-2022-38627 (Linear eMerge)**: physical access control systems.
  - **CVE-2024-12856 and CVE-2024-9644 (Four-Faith)**: industrial routers.
  - **CVE-2021-46417 (Franklin Fueling Systems Colibri Controller Module)**.
- **Three OT vulnerabilities were added to CISA KEV after we reported attacks on the AEE**:
  - **CVE-2018-4063 (Sierra Wireless)**: added after our blog on attacks against industrial routers.
  - **CVE-2021-26828 and CVE-2021-26829 (OpenPLC ScadaBR)**: added after our blog detailing a hacktivist attack on our HMI.

Insight for defenders: When deciding what to patch, and when, prioritize evidence of active exploitation alongside CVSS and other severity metrics. The CISA KEV catalog is a valuable baseline, but it does not capture the full exploited vulnerability landscape. Use additional threat intelligence to prioritize vulnerability risk mitigation, including Vedere Labs' threat feeds and other trusted sources.

2.6. OT Attacks: Modbus is the Undisputed Leader

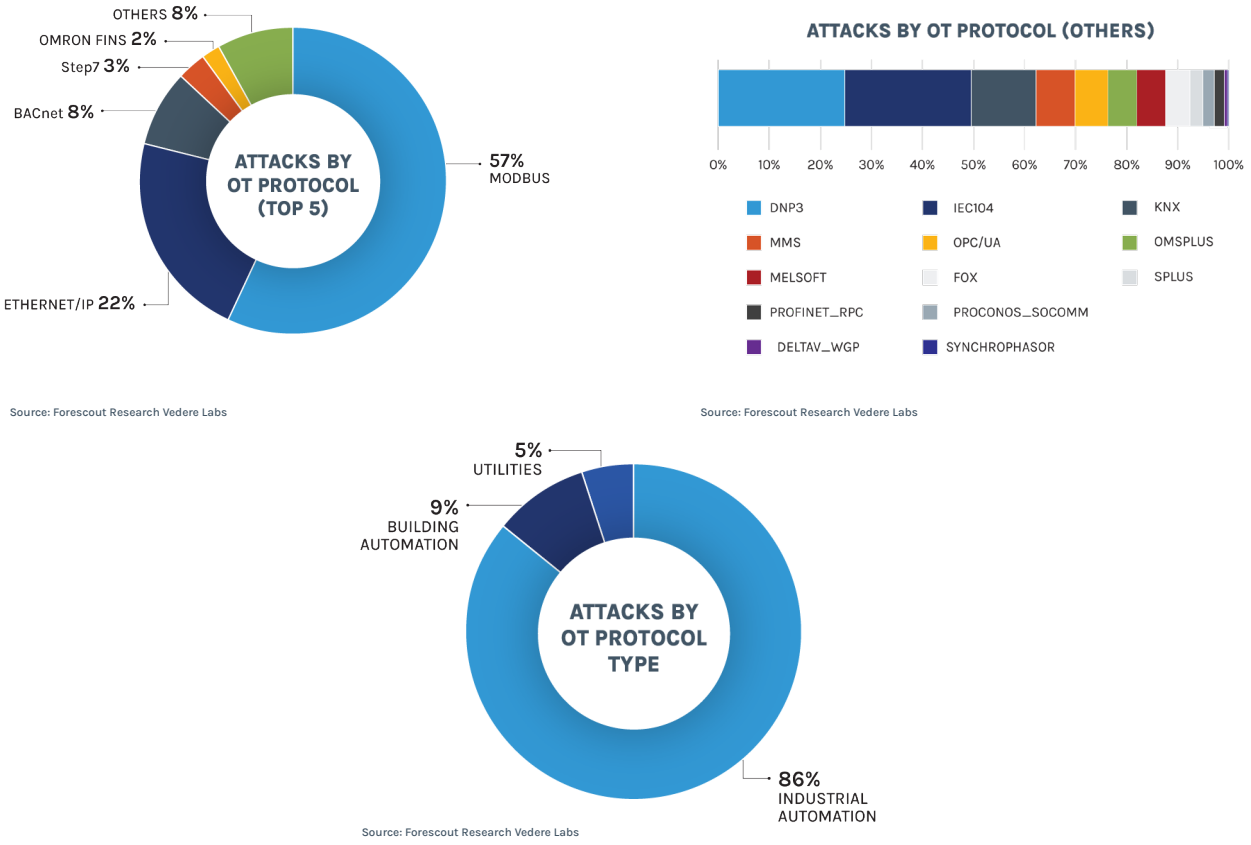


Figure 6 – Attacks against OT protocol

Figure 6 shows the distribution of attacks targeting OT protocols. **Overall, attacks on OT protocols grew by 84% in 2025**. As in 2024, five protocols accounted for the largest share of observed activity:

- **Modbus:** the most popular and most often exposed, OT protocol, **accounted for 57% of OT attacks in 2025, up from 40% in 2024**.
- **EtherNet/IP**: 22% in 2025, down from 28% in 2024.
- **BACnet**: 8% in 2025. Used in building automation, it moved from fifth most targeted in 2024 to third in 2025.
- **Step7**: 3% in 2025 down from 8% in 2024, and it shifted from fifth to fourth in the rankings.
- **Factory Interface Network Service (FINS)**: replaced DNP3 as the fifth most targeted protocol in 2025. FINS is used by OMRON systems, while DNP3 is commonly used in utilities.

The "other protocols" category remained stable at 8% in 2025, down from 9% in 2024. The top list was broadly similar to 2024, with two additions: OMS+ (Siemens S7) and PROFINET RPC.

By protocol category, **attacks on industrial automation protocols increased to 86% in 2025**, up from 79% in 2024, driven primarily by increased Modbus activity. Utility protocols continued to decline, dropping to 5% from 12% in 2024, while building automation remained stable at 9%. Because utilities declined, building automation is now the second most targeted category by share. In absolute terms, **attacks against building automation protocols increased by 33% in 2025**.

Overall, the data shows sustained focus on Modbus, with more fragmented activity across other protocols. Defenders should not limit monitoring to only the "popular" protocols with the most widely available tooling.

Insight for defenders: Monitoring traffic to and from OT assets is now as critical as monitoring IT traffic. Attackers are continuously probing these assets for weaknesses, and many organizations remain blind because they lack visibility into OT environments. Building automation protocols, and even widely deployed protocols, such as Modbus, are present in many organizations and should be treated as high-priority targets for risk monitoring and risk reduction.

2.7. Attacker Actions and TTPs: Discovery Continues to Dominate

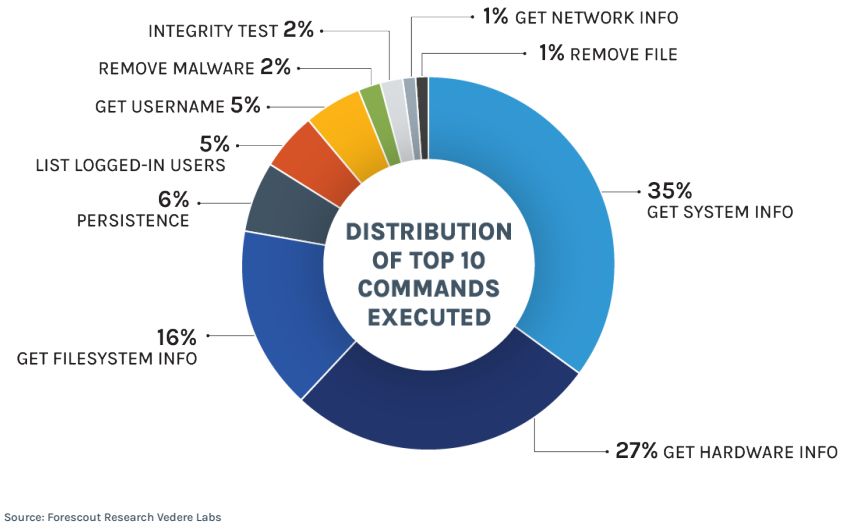


Figure 7 – Top executed commands

Figure 7 shows the distribution of the top 10 commands executed, primarily over SSH or Telnet, after attackers gained initial access. Most of the activity we observed was automated and mapped to the following MITRE ATT&CK tactics:

TA0007 — Discovery: 91% in 2025, up from 84% in 2024, and 25% in 2023.
- System reconnaissance: CPU, RAM, file system, OS, and architecture.
- User enumeration: logged-in users, running processes, and scheduled jobs.
- **Attackers are spending more time exploring before taking action.**

TA0003 — Persistence: 6% in 2025, down from 12% in 2024.
- SSH key installation.
- Backdoored shell deployment.

- User account creation and manipulation.
- Background process execution.

TA0002 — Execution: 3% in 2025, down from 4% in 2024.
- File system interaction.
- Malware download and execution.

The continued increase in discovery activity suggests that attackers are spending more time interacting with a breached system before moving on. This may be to understand what is present on the asset or to identify additional opportunities in the environment. One notable pattern we observed in 2025 was automated activity searching for Telegram data for exfiltration, a behavior also described by other researchers.

Insight for Defenders: Increased time spent on discovery creates more opportunities for detection before they take higher impact actions, such as data exfiltration, deletion, or encryption. Organizations should prioritize the ability to detect discovery behavior early, using endpoint telemetry for system discovery and network signals for lateral and network discovery activity.

2.8. Malware: Everything Remains as It Never Was

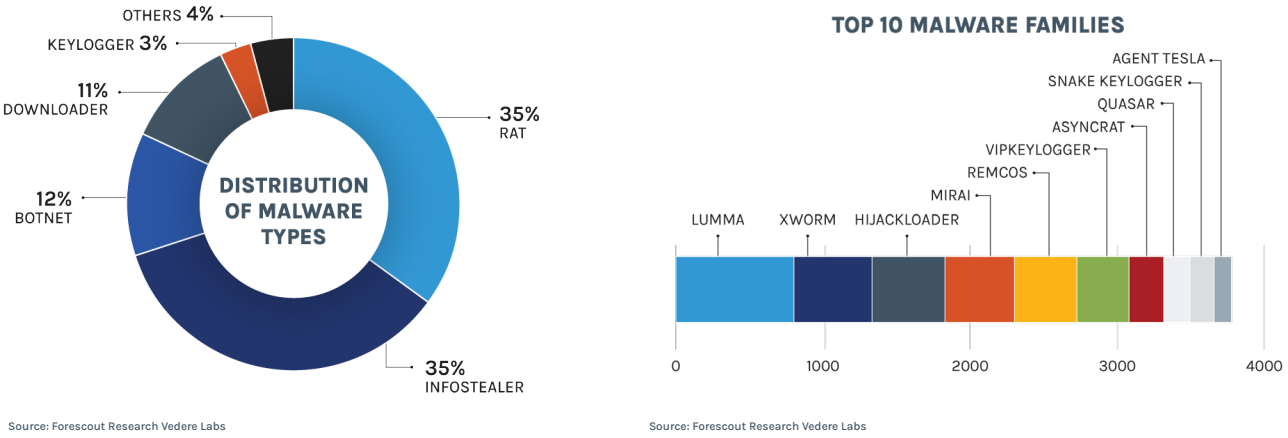


Figure 8 – Distribution of observed malware samples and C2 servers

Figure 8 shows the distribution of malware in our dataset. Remote access trojans (RATs) and infostealers were tied for first place in 2025 with botnets in second.

These three categories typically dominate because they underpin much of cybercriminal activity. In 2024, they accounted for 85% of observed malware, and in 2025, that share declined slightly to 82%. The most notable shift was in botnets which fell from 29% in 2024 to 12% in 2025. Over the same period, RATs increased from 27% to 35% and infostealers increased from 29% to 35%. Downloaders also grew materially rising from 4% in 2024 to 11% in 2025. The “Others” category includes cryptominers, ransomware, worms, and other malware families. Overall, the category-level distribution suggests continuity rather than a major structural shift.

The picture changes when we look at specific families. Six of the most prevalent malware families in 2025 did not appear in the 2024 top list, indicating rapid turnover. The rise of modular, multi-capability malware (XWorm and

HijackLoader) and the widespread abuse of open-source tools (AsyncRAT and Quasar) suggests attackers favor versatile, readily available frameworks over single-purpose malware.

Multi-Function Threats

XWorm: second most common family in 2025.

- Timeline: first seen in 2022, abandoned in 2024, and re-advertised on hackforums[.]net in June 2025.
- Capabilities: modular toolkit with RAT, infostealer, and ransomware functionality.
- Status: Rapidly gaining popularity after its relaunch.

HijackLoader: also known as IDATLoader, DOILoader, SHADOWLADDER, and GHOSTPULSE.

- Timeline: active since 2023.
- Capabilities: modular loader focused on code injection, execution, and defense evasion.
- Notes: similar multi-module approach to XWorm.

Infostealers

VIP Keylogger: new variant.

- Timeline: first observed in late 2024.
- Origin: derived from Snake Keylogger.
- Growth driver: Lumma stealer decline.

Snake Keylogger: also known as 404 Keylogger.

- Timeline: active since 2019.
- Business model: subscription based.
- Growth driver: Lumma stealer decline.

Context: Lumma Stealer's disruption

Despite remaining the most prevalent infostealer in 2025, Lumma faced early-year disruptions and later Telegram account compromises and member doxxing, creating space for alternatives such as VIP Keylogger and Snake Keylogger.

Open-Source RATs

AsyncRAT: .NET-based, GitHub-hosted.

- Development: active from 2019 to 2023.
- Distribution: packaged in compromised software installers.
- Developer claim: "Not intended for malicious use," widely ignored by threat actors.

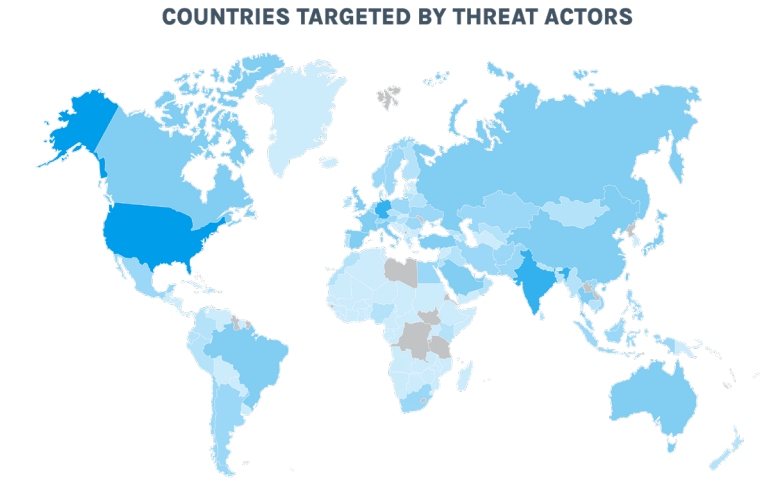
Quasar: .NET-based, GitHub-hosted.

- Development: active from 2016 to 2023.
- Status: remains popular despite inactive development.
- Distribution: widely adopted by threat actors.

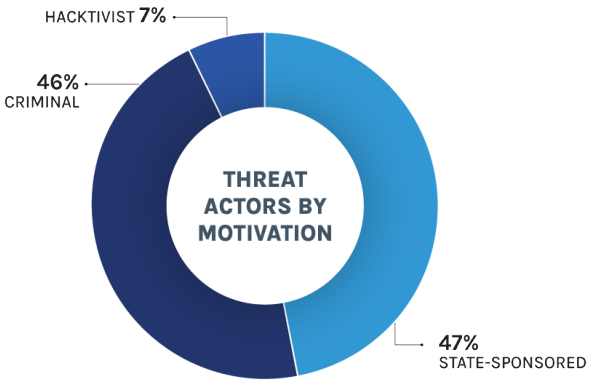


Insight for defenders: Malware families and samples evolve continuously, but the underlying operating model remains consistent. Attackers continue to rely on a familiar ecosystem of RATs, infostealers, botnets, and shifting C2 infrastructure. As a result, detection and hunting are typically more effective when focused on TTPs and anomalous behavior than when they rely solely on file hashes and C2 IPs, which change frequently.

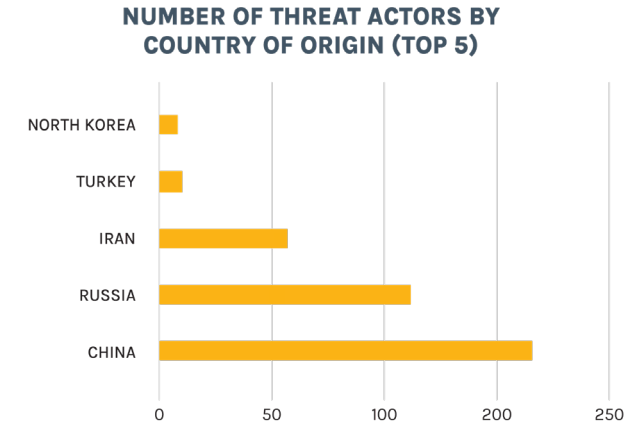
2.9. Threat actors: Focus on Critical Infrastructure



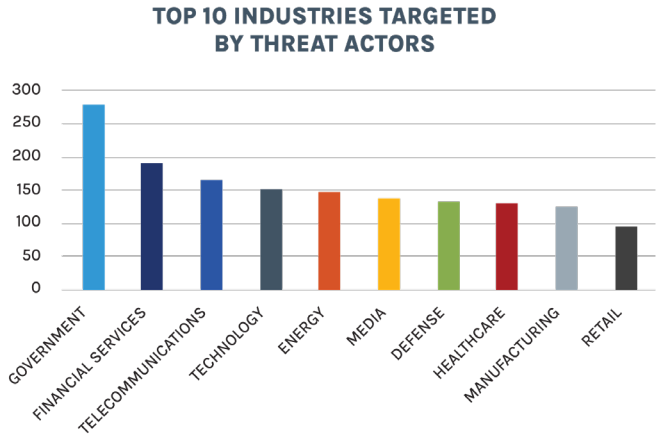
Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

Figure 9 – Distribution of threat actors

Vedere Labs maintains a database of almost 900 threat actors, up 10% from 2024. The database includes:

- **Cybercriminals:** 46% in 2025, up from 45% in 2024.
- **State-sponsored actors:** 47% in 2025, down from 48% in 2024.
- **Hacktivists:** 7% in 2025, unchanged from 2024.

Figure 9 shows how these actors were distributed in 2025 by origin and targets:

- Threat actors targeted 178 countries in 2025, up two from 2024.
- The United States remained the most targeted, with 276 actor groups, up 12 from 2024.
- India ranked second, with 154 groups, followed by Germany with 149.
- Threat actors were associated with 45 origin countries in 2025.
- The largest share of actor groups was associated with China (210), Russia (112), and Iran (55).
- Combined, these three countries accounted for 45% of threat actor groups.
- Government, financial services, and telecommunications were the most targeted industries, unchanged from 2024.

In 2025, we analyzed campaigns from China-linked threat actors targeting medical systems and enterprise software. Other researchers also reported continued activity against small office and home office (SOHO) routers to build proxy botnets, as well as ongoing targeting of telecommunications and critical infrastructure providers. Together, these patterns reinforce a continued focus on both espionage and infrastructure exploitation.

Russia- and Iran-linked activity also included hacktivist-style personas, such as NoName057(16) and Handala Group, which we analyzed in a recent report. These groups often emphasize disruptive messaging and infrastructure impact and align operations with geopolitical flashpoints. On June 30, 2025, CISA, the FBI, and the NSA issued a joint alert warning of the potential for increased targeting of United States critical infrastructure by Iran-linked actors. On December 9, 2025, CISA and international partners released an advisory related to Russia-linked hacktivists.

Because critical infrastructure sectors remain among the most targeted, we drill down into five sectors in 2025: healthcare, financial services, government, manufacturing, and energy. The following figures summarize the threat actor groups targeting each sector, including likely motivation, and the most common origin countries. The same overall patterns from last year remain, with changes primarily in year-over-year growth by industry.

Motivations Drive Actor Types

Cybercriminals dominate healthcare, financial services, manufacturing.

- Motivation: high-value data and ransom potential.
- Target preference: organizations more likely to pay rather than risk operational downtime.

State-sponsored actors dominate government and energy.

- Motivation: espionage, pre-positioning for future conflict, and potential for physical disruption.
- Strategic value prioritized over immediate financial gain.

Hacktivists concentrate on government.

- Motivation: geopolitical alignment and messaging.

Geographic Origin Patterns

- **Universal presence:** China, Russia, Iran, and North Korea appear in the top five origin countries across all five sectors.

- **Regional specialists**
  - Brazil: financial services and energy.
  - India: government and manufacturing.

2025 Growth by Sector

Threat actor counts increased most in 2025 in:

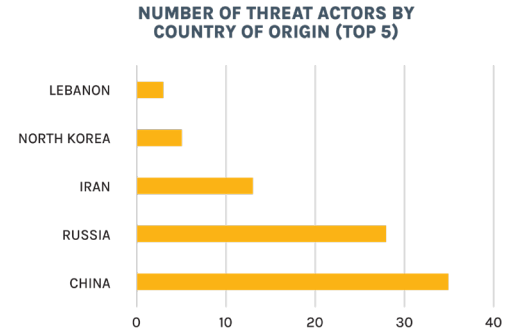
1. **Manufacturing: 16% in 2025,** the highest growth.
2. **Healthcare: 13%.**
3. **Government: 6%.**
4. **Energy: 6%.**
5. **Financial services: 5%.**

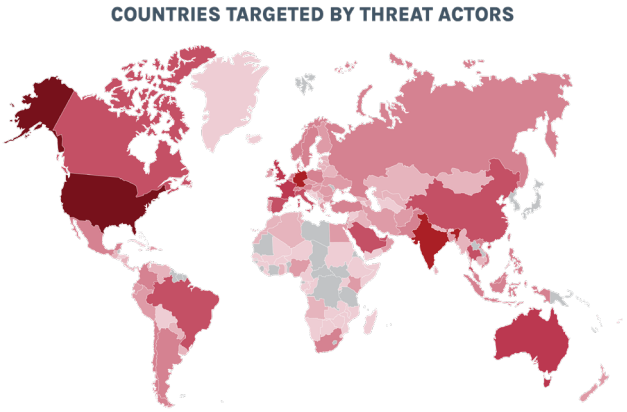
Healthcare

Total number of threat actors:

130

(+13% from 2024)







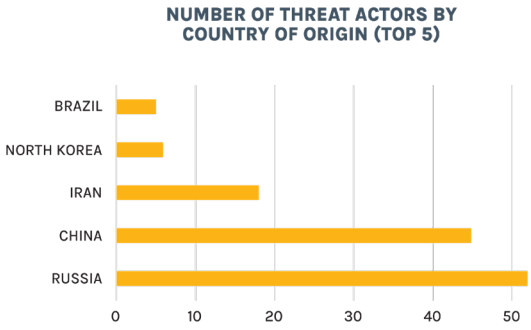
Source: Forescout Research Vedere Labs

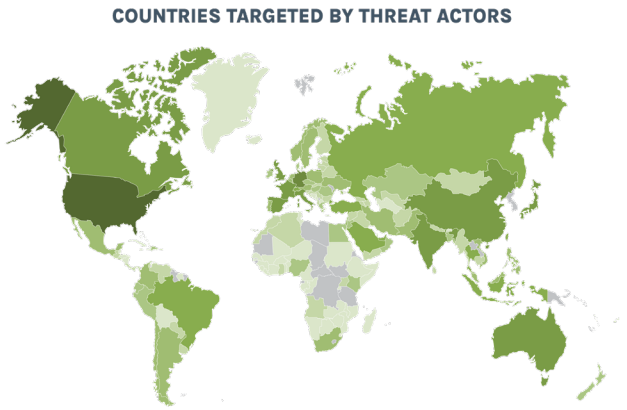
Financial Services

Total number of threat actors:

190

(+5% from 2024)







Source: Forescout Research Vedere Labs

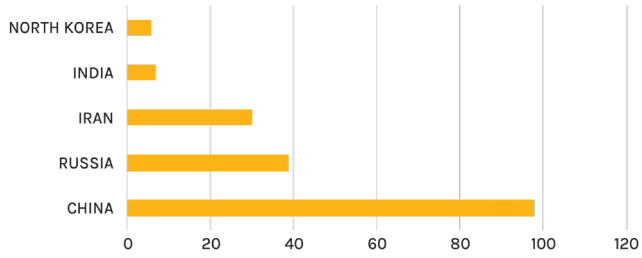
Government

Total number of threat actors:

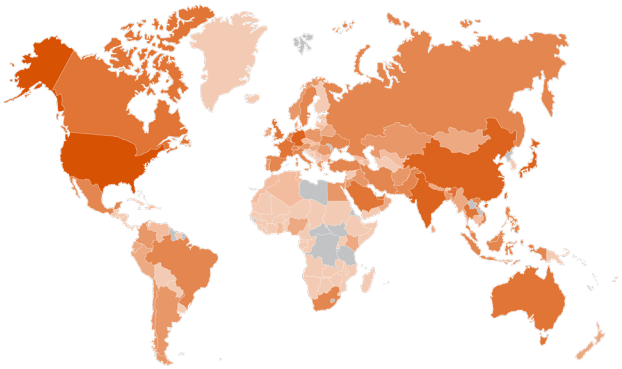
278

(+6% from 2024)

NUMBER OF THREAT ACTORS BY COUNTRY OF ORIGIN (TOP 5)



COUNTRIES TARGETED BY THREAT ACTORS





Source: Forescout Research Vedere Labs

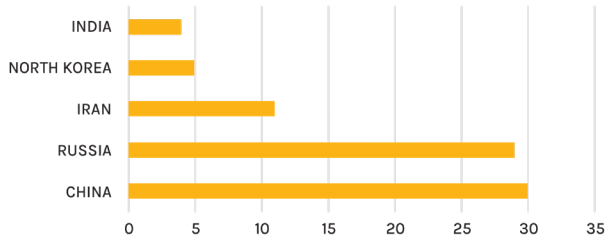
Manufacturing

Total number of threat actors:

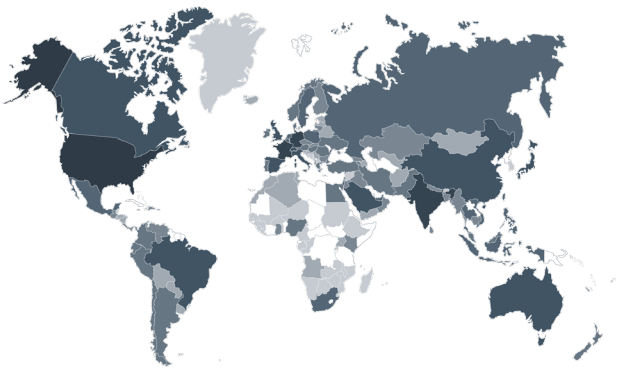
125

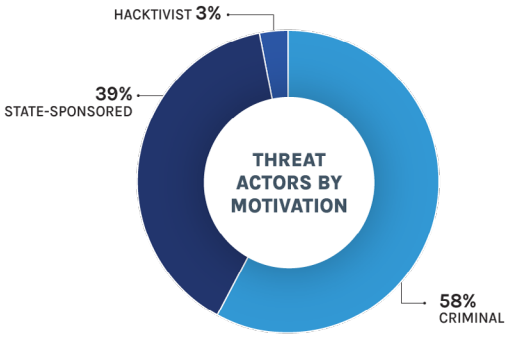
(+16% from 2024)

NUMBER OF THREAT ACTORS BY COUNTRY OF ORIGIN (TOP 5)



COUNTRIES TARGETED BY THREAT ACTORS





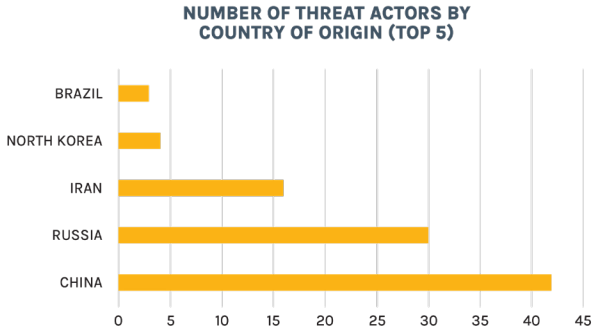
Source: Forescout Research Vedere Labs

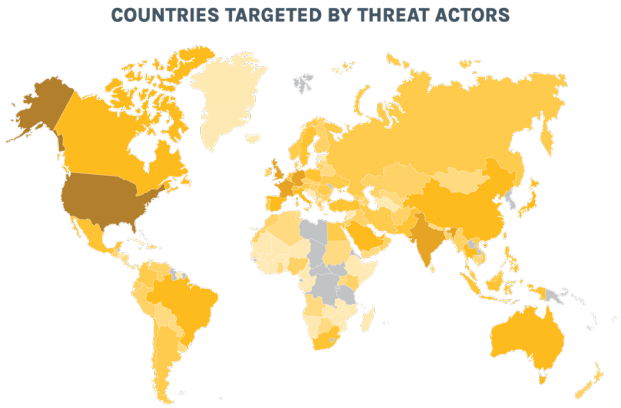
Energy

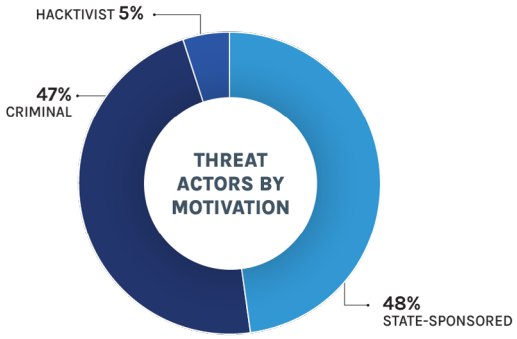
Total number of threat actors:

147

(+6% from 2024)







Source: Forescout Research Vedere Labs

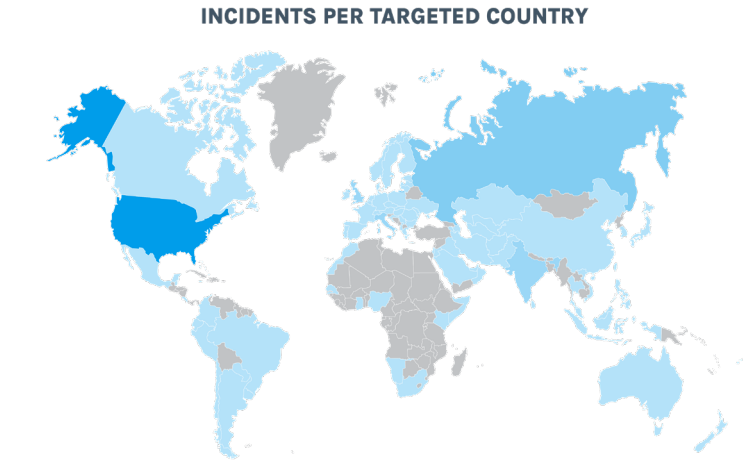
Insight for defenders: Blocking communications solely by country is rarely effective, and origin attribution alone is not always the most actionable input. However, understanding threat actor goals and sector targeting can help prioritize strategic security investments. Organizations in heavily targeted industries should monitor current threat intelligence for sector-specific campaigns and adjust detection and response priorities accordingly.

2.10. Incidents and Data Breaches: Cybercrime Is Widespread

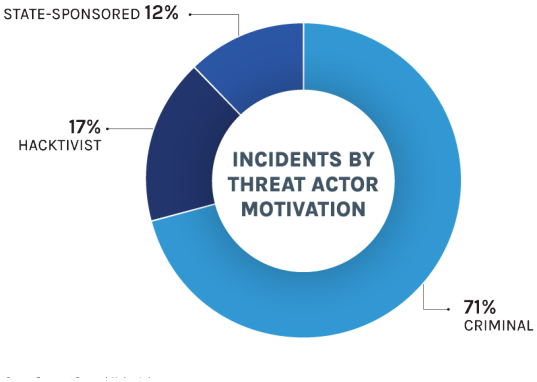
To report statistics on publicly disclosed cyber incidents, we use the Cyber Events Database maintained by the Center for International and Security Studies at the University of Maryland (CISSM). The database catalogs publicly reported cyber events. We do not compare these incident results with previous years because we used a different source in our 2024 report. In addition, the Cyber Events Database snapshot used here only includes records through November 30, 2025, and totals may change as additional incidents are added.

The database recorded 1,189 incidents across 95 countries. The results, shown in Figure 10, broadly align with the threat actor distribution in Section 2.9, with several differences:

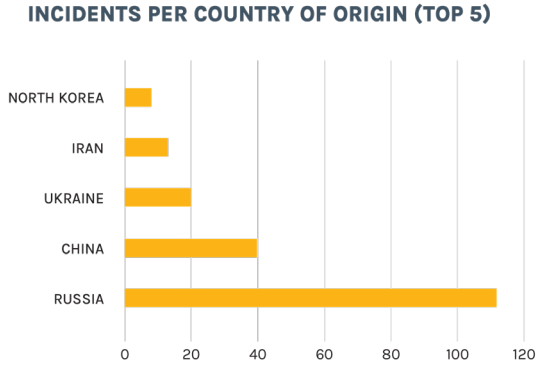
- Although China is associated with more threat actor groups, Russia had a higher number of recorded incidents.
- Ukraine ranked third by incident volume, reflecting its ongoing conflict with Russia.
- Even though the number of cybercriminal and state-sponsored groups is similar (Section 2.9), cybercriminals were responsible for nearly six times more incidents.
- Critical infrastructure sectors were not only heavily targeted by threat actor groups but also experienced the highest incident volumes. Government ranked first in both views, while healthcare had relatively fewer associated actor groups, but a higher incident count.



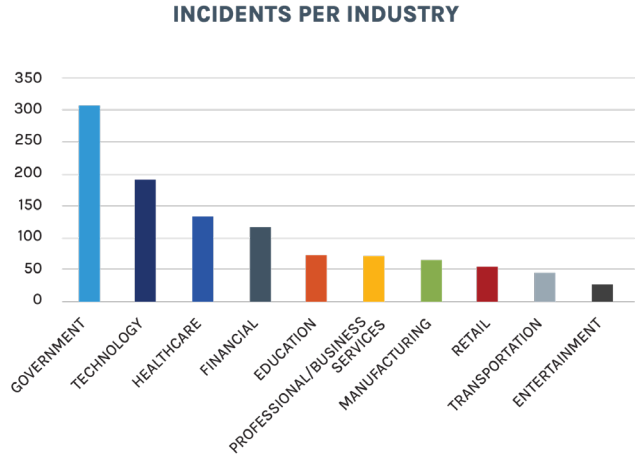
Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

Figure 10 – Distribution of incidents

In May 2025, we published a study showing how healthcare organizations were the ones suffering most data breaches and were the most likely to experience multiple breaches. Because of the impact on patient safety and organizational resilience, we extended our healthcare breach analysis to cover 2025 through December 18, 2025, using the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Breach Portal. The portal lists breaches of unsecured protected health information affecting 500 or more individuals, as required by U.S. law.

As of December 18, 2025, 622 healthcare data breaches were reported on the OCR Breach Portal. Of these, 133 were archived and 489 remained under investigation.

These breaches affected a combined 44,781,525 individuals, with an average of 71,996 individuals per breach. Eight incidents each affected more than one million people.

Figure 11 breaks down healthcare breaches by affected entity, type, and location of compromised information. Notably, **80% of these breaches were attributed to "hacking/IT incidents."** This aligns with the trend we highlighted last year, showing the dramatic rise in such incidents from 0% in 2009 to nearly 80% by 2024.

Take note: **Nearly 60% of all healthcare breaches, 59%, involved data stored on network servers. This underscores the need to treat servers as critical assets in healthcare environments *and* to prioritize their protection to reduce the likelihood and impact of future breaches.**

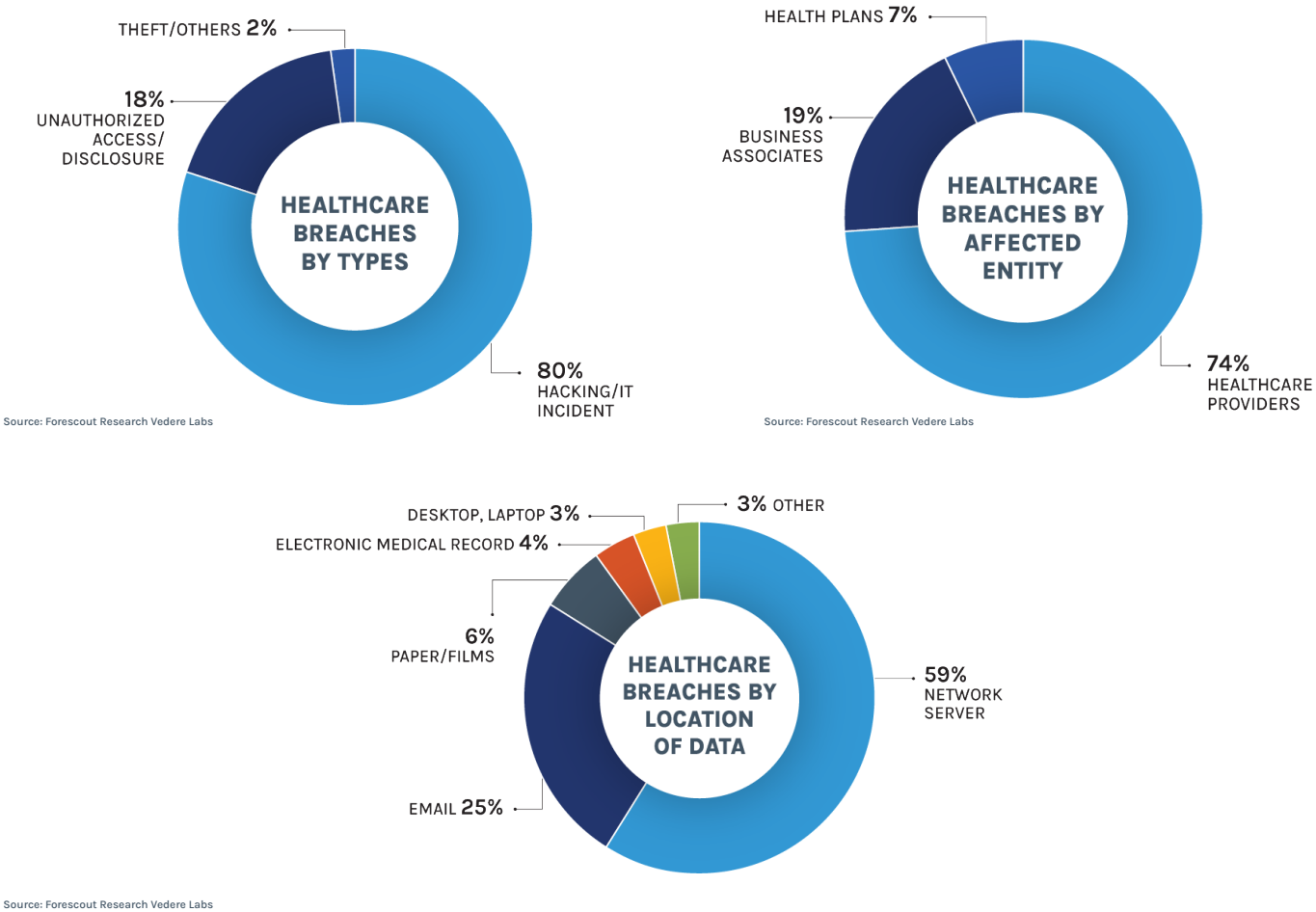


Figure 11 – Distribution of healthcare breaches

3. Mitigation Recommendations

In this report, we analyzed data related to the attacks, exploits, malware, threat actors, and incidents we observed in 2025. Throughout the report, we included “Insight for defenders” guidance alongside each main finding.

Organizations should **prioritize extending** visibility**,** risk assessment **and** proactive controls **across an expanding attack surface, including network perimeter assets, operational technology environments, healthcare systems, and IoT assets**.

At a minimum, organizations should:

- Ensure full visibility into these assets, including their presence on the network, the software they run, and their communication patterns. This can be achieved at scale with agentless solutions.
- Understand asset risk profiles across vulnerabilities, weak configurations, exposure and other factors.
- Disable unused services and patch vulnerabilities to reduce the window of exploitation.
- Change default or easily guessable credentials and use strong, unique passwords for each asset.
- Enforce multifactor Authentication (MFA) whenever possible, especially for VPN access.
- Encrypt sensitive data in transit and at rest, especially personally identifiable information (PII), protected health information (PHI), and financial data.
- Avoid exposing unmanaged or legacy assets directly to the internet unless absolutely necessary. Where exposure is required, ensure administrative interfaces, such as web UIs and engineering ports, require authentication and are secured behind IP-based access control lists or a VPN-protected management VLAN.
- Apply IP-based access control lists to limit access to sensitive protocols, such as Modbus and BACnet, in OT networks.
- Segment the network to isolate IT, IoT and OT assets, limiting network connections to only authorized management and engineering workstations or to the minimum set of asset-to-asset communications required for operations. Segmentation also helps prevent lateral movement using compromised credentials.

Informed by our 2025 research, we also recommend the following enhanced measures:

- Enable endpoint logging beyond alerts to include process, file, user, network, registry, driver and PowerShell activity.
- Collect logs from systems that handle user authentication, especially SSO and cloud service access.
- Deploy continuous monitoring for suspicious authentication attempts and routinely review logs for signs of unauthorized access.
- Rotate credentials and cryptographic keys suspected of compromise.
- Block suspicious top-level domains (TLDs) associated with infostealer infrastructure.
- Implement browser security controls to reduce the risk of credential theft.
- Conduct targeted training on social engineering techniques.

Once these controls are in place, ensure threat detection and response coverage spans the entire organization, including every asset type. Modern threats frequently move across asset classes, so it is critical to detect activity end-to-end, from an initial foothold, such as a vulnerable router, to a pivot point, such as a misconfigured workstation, to a final target, such as an exposed OT asset. Ensure your threat detection solution covers all asset types and ingests telemetry from multiple sources, including firewalls, intrusion detection systems, endpoint detection and response, and other existing security infrastructure.

© 2026 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products or service names may be trademarks or service marks of their respective owners.