2024 Global Threat Roundup Report

January 27, 2025

FORESCOUT RESEARCH | VEDERE LABS

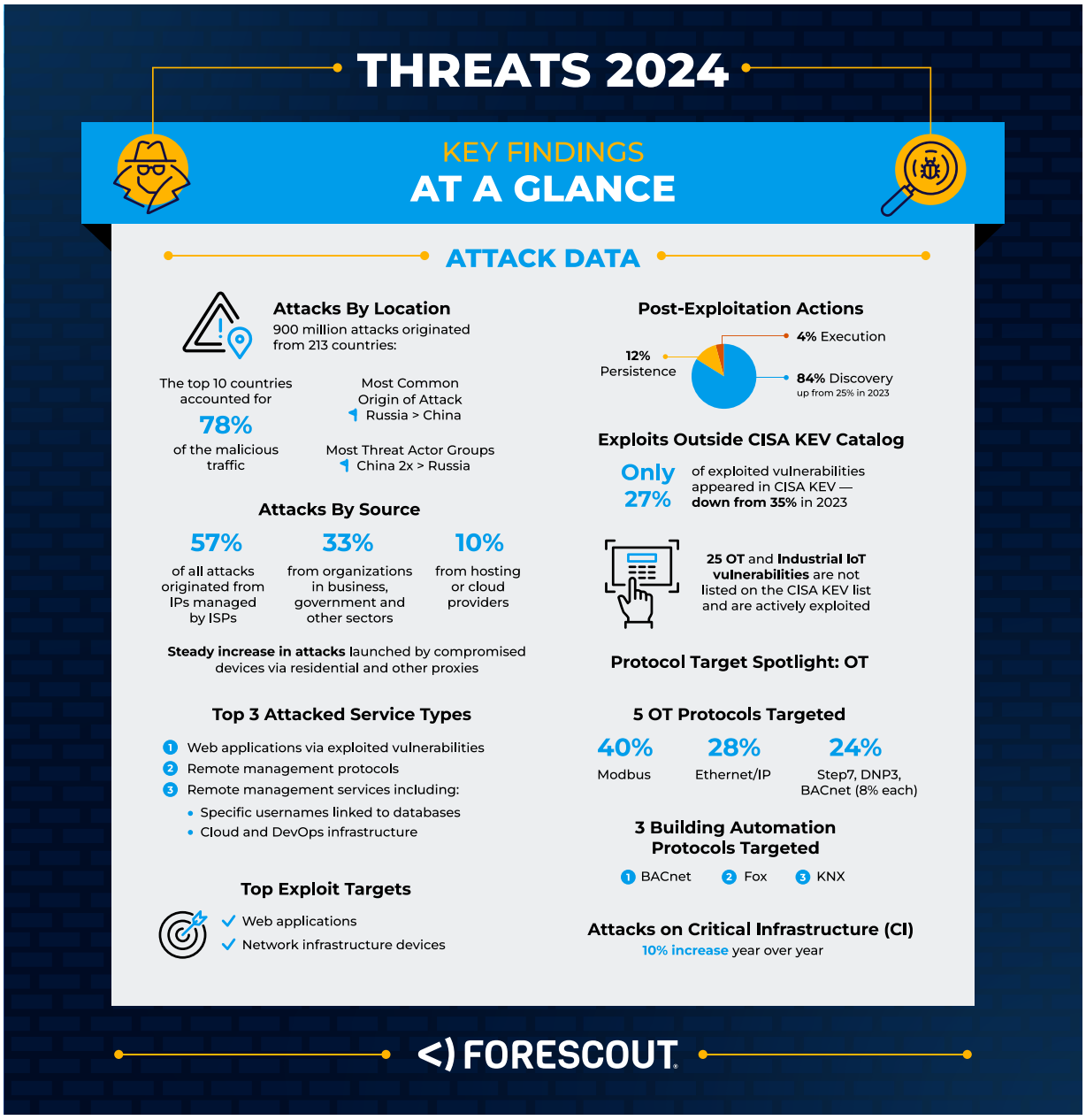
Contents

1. Executive Summary

From the financial impact of attacks to geopolitical tensions that lead to cyber warfare, cybersecurity is top of mind for enterprise and government organizations in 2025. In this report, we look back at the **900 million attacks** we analyzed in the threat landscape of 2024. Additionally, we offer organizations tactical insights and strategic recommendations for improving defenses this year.

Cyber attacks are on the rise once again – including an uptick of targets in critical infrastructure in the last year. Since 2022, however, reported incidents in critical infrastructure rose from 50 to 384 globally – or 668%, according to data from the European Repository of Cyber Incidents, an independent research consortium that provides scientific analysis of cyber incidents.

Take note: We also include information on vulnerabilities and exploits that are not on the CISA-KEV list but are being exploited today.



THREATS 2024

KEY FINDINGS AT A GLANCE

ATTACK DATA

Reported CI Incidents

2022	2023	2024
50	349	384

% of All Incidents Targeting CI Sectors

2022	2023	2024
34%	58%	57%

Top CI Incidents by Region:

1. North America (U.S.)
2. Europe (Germany, France, Spain, Italy, UK)
3. Asia (Japan, India, Korea, Taiwan, Singapore)

CI Incidents by # of Countries Affected

2022	2023	2024
27	57	79

THREAT ACTOR DATA

Number of Threat Actors

A **majority (43%)** of all threat actor groups are based in:

1 China	2 Russia	3 Iran
199	98	55

Top 3 Countries Targeted by the Most Threat Actors

1 United States	2 Germany	3 India
264	144	141

Top 3 Verticals Targeted by Threat Actors

384	349	50
Telecommunications	Financial Services	Government

Threat Actor Increase (YoY):

93%	71%	55%
Energy	Manufacturing	Healthcare

MALWARE

Top 3 by Type:

29%	29%	27%
Botnets	Information stealers	Remote Access Trojans/C2

Most Common C2:

1. Cobalt Strike
2. Viper
3. Sliver

Most Common Botnet:

Mirai

Most Common Infostealer:

Lumma stealer

FORESCOUT

Where Does Our Data Come From?

Most data used for our analysis comes from the Vedere Labs **Adversary Engagement Environment (AEE)**, a set of honeypots on the open internet luring attackers and recording their interactions. Data points in the AEE are called attacks. They can represent a multitude of malicious actions, including port scanning and brute forcing. The AEE recorded more than 900 million attacks between January and December 2024. A subset of these attacks contains exploits – attempts to exploit vulnerabilities.

Our data differs from what is seen in many other threat reports because it comes from specialized IT/OT/IoT honeypots that either mimic realistic device profiles – including exposed protocols, banners and parts of the filesystem – or are real specialized devices, instead of generic honeypots capturing every kind of attack.

Our Malware Analysis Lab (MAL) collects and analyzes samples dropped by attackers on the AEE or shared on public repositories. Our goal is not to analyze as many samples as possible, but to focus on those that are unique. **We analyzed more than 100,000 unique malware samples between January and December 2024.**

Also, we constantly hunt for new command and control (C2) infrastructure and maintain a threat actor knowledgebase with **data about more than 800 threat actors.**

2. Main Findings

2.1. Location – Russia Retakes China's Position

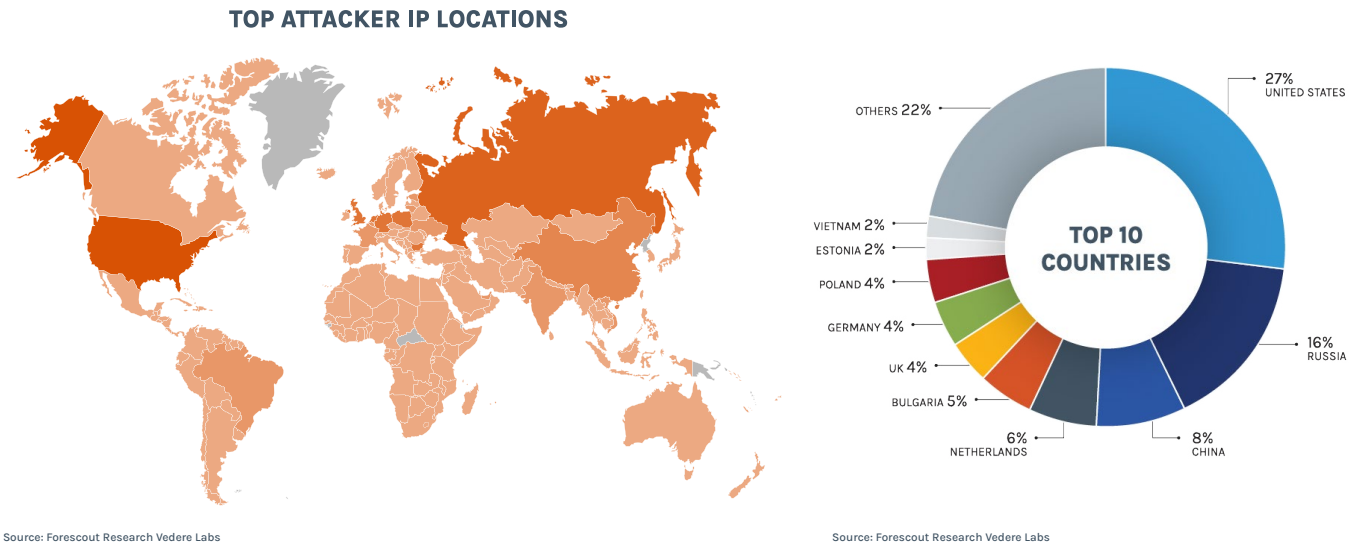


Figure 1 – Distribution of attacks by IP address country of origin

Figure 1 shows the distribution of attacks detected by country of origin. We detected attacks originating from 213 countries and territories (1 more than in 2023 and 22 more than in 2022). Countries appear in this list due to the presence of legitimate hosting providers being abused by attackers; the presence of bulletproof hosting providers that cater specifically to cybercriminal activities; or the use of compromised hosts to launch attacks.

This year, the top 10 countries accounted for 78% of the malicious traffic. This is a negligible difference of 1% more than in 2023 but consistent with the growth observed since 2022 (73%). The top 10 list of countries originating attacks has only one entry different from 2023: Poland replaced Singapore. However, the ranks have changed considerably. The most notable change: Russia rose from 9% to 16% of attacks. China decreased from 18% to 8%.

It is important to stress that it is not direct attribution for attack locations. It is only where we can see attacks coming from as they hit our honeypots. Our threat actor database shows that most actors are still located in China — although it does not necessarily mean it is the source of individual attacks.

Fact: China and Russia have been in the top 3 of IP address attack origin since 2022.

Insight for Defenders: Country of origin alone continues to be ineffective to judge the risk of a particular IP address. However, if your organization does not do business with – or in – countries with the highest number of IP addresses that attack, blocking those IP ranges may help reduce SOC noise.

2.2. Autonomous Systems – New Techniques for Routing Attacks

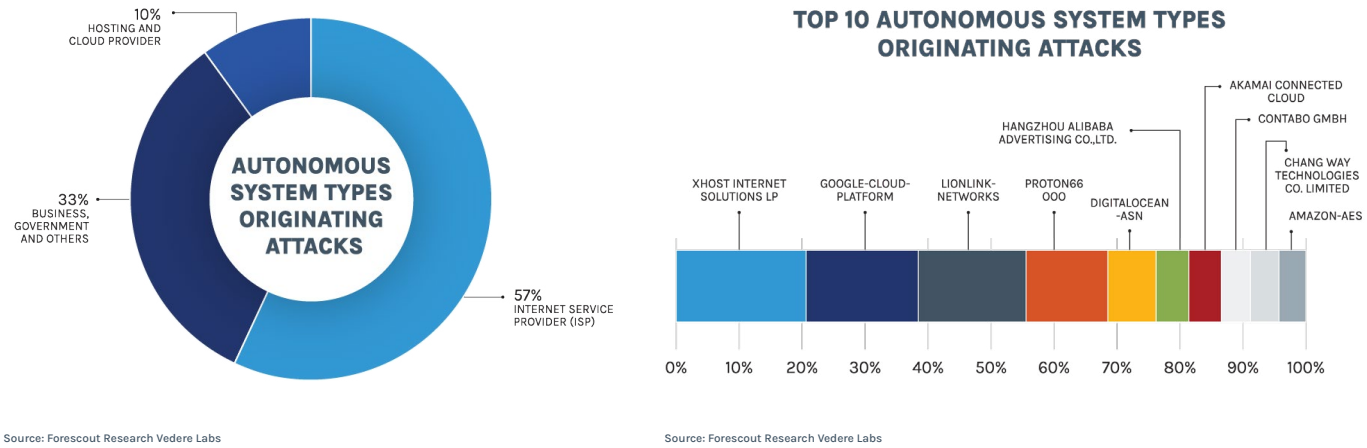


Figure 2 – Distribution of attacks by originating Autonomous System

Attacks again originated from more than 500 autonomous systems (AS), which are blocks of IP addresses under the control of an organization. Figure 2 shows the percentage of attacks coming from the three types of AS we observe:

- Internet Service Providers (ISPs) increased from 53% in 2023 to 57% in 2024
- Business, Government, and others decreased from 36% to 33%.
- Hosting or cloud providers decreased from to 11% to 10%.

Note that the percentages shown above differ from what was presented in last year's report because we removed the "unknown" category of AS and only show the numbers of those we can classify.

As we discussed last year, the large chunk of attacks coming from ISPs as well as business, government and other organizations signifies an increase in the use of compromised devices to launch attacks as opposed to leasing infrastructure from dedicated providers.

In 2023, we attributed this to the increased popularity of "residential proxy" services, where threat actors proxy their traffic via applications running on residential devices, which typically have IP addresses managed by ISPs. Residential proxies continue to be popular, with emerging threat actors specializing in selling access to hijacked IoT devices for this very purpose, something we predicted in early 2023. However, advanced persistent threat actors have now gone even further and developed Operational Relay Boxes (ORB) networks, where they mix virtual private servers, compromised IoT and hijacked network perimeter devices, creating layers of proxying to make detection and attribution of attacks more challenging.

On the cloud side, the use of Amazon and Google infrastructure continued to be significant, with those two alone accounting for more than 11% of the attacks we observed. A notable change was that the major Chinese cloud provider Alibaba jumped from 22nd most popular AS in 2023 to sixth in 2024.

Overall, the top 10 ASes are responsible for 48% of attacks (4% less than in 2023). Six ASes from the top 10 in 2023 remain in the list in 2024: Xhost Internet Solutions Lp, GOOGLE-CLOUD-PLATFORM, LIONLINK-NETWORKS, DIGITALOCEAN-ASN, Contabo GmbH and Chang Way Technologies Co. Limited.

Fact: Autonomous Systems continue to be a better sign of risk than country of origin.

Insight for Defenders: IPs belonging to known risky autonomous systems should always be treated with care — especially those that remain in the top 10 for years, such as Digital Ocean. Continued attacker interest in compromised devices to route action shows organizations need real-time threat intelligence about compromised devices in the wild and the types of device attackers focus on. This goes beyond APTs targeting a specific organization. Be wary of opportunistic Initial Access Brokers (IAB) that breach as many organizations as possible and sell that access.

2.3. Attacked Services – the Web Is the Undisputed Leader

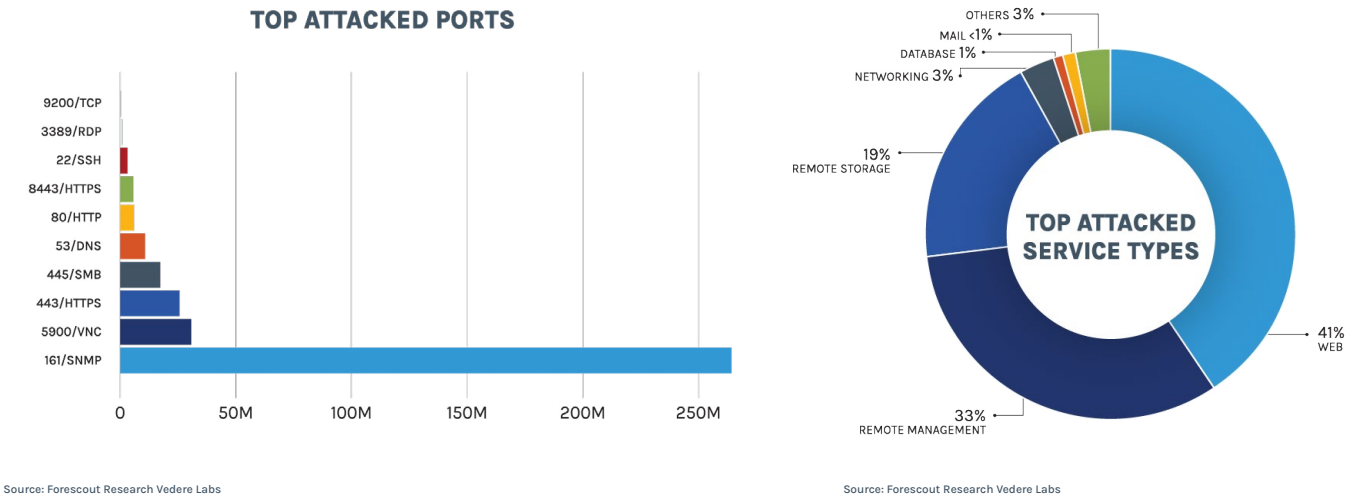


Figure 3 – Distribution of attacked ports and services

Figure 3 shows the share of traffic targeting each type of network service, classified according to assigned or well- known IPv4 TCP destination ports: Web applications increased from 26% in 2022 and 2023 to 41% in 2024, continuing to be the most attacked service type and widening with the gap with the other targets. Most attacks against these services are either scanning or attempts at vulnerability exploitation (see section 2.5).

Remote management protocols, such as RDP and VNC for remote desktop, and SSH and Telnet for remote terminals, increased from 26% in 2023 to 33% this year. It was 43% in 2022. Attacks on these protocols are mainly brute forcing or password spraying (see section 2.4).

Remote storage protocols, such as SMB and FTP, remained relatively stable, changing from 20% to 19%, continuing their decrease from 23% in 2022. Networking protocols, such as DNS, DHCP and CWMP/TR-069, decreased from 10% to 3%, returning to the baseline in 2022 of 1%.

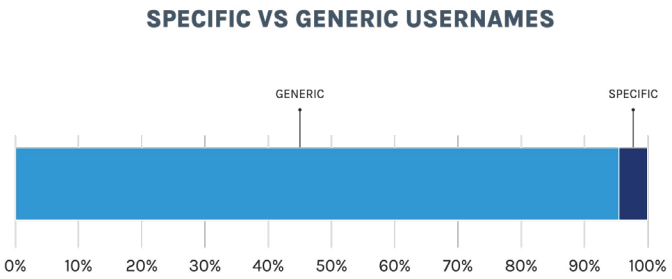
Database services, such as Microsoft SQL Server, Redis, mongoDB, MySQL and PostgreSQL, decreased from 6% to 1%, returning to 2022 levels.

E-mail services, such as IMAP, POP3 and SMTP, remained unchanged since 2022 at less than 1% of attacks.

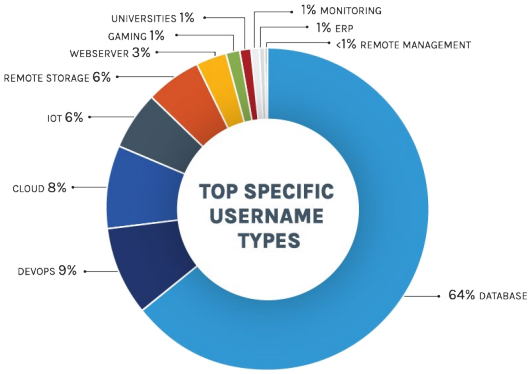
Fact: Web applications are, without a doubt, the most attacked service type, continuing the trend from 2023.

Insight for Defenders: Ensure that defenses, such as web application firewalls, are in place to detect and prevent attacks such as command injections, cross-site scripting and SQL injections as early as possible. The increase in attacks on remote management protocols is also significant because most of those are related to credential-based attacks. Best practices in credentials are paramount, such as avoiding default and easily guessed passwords.

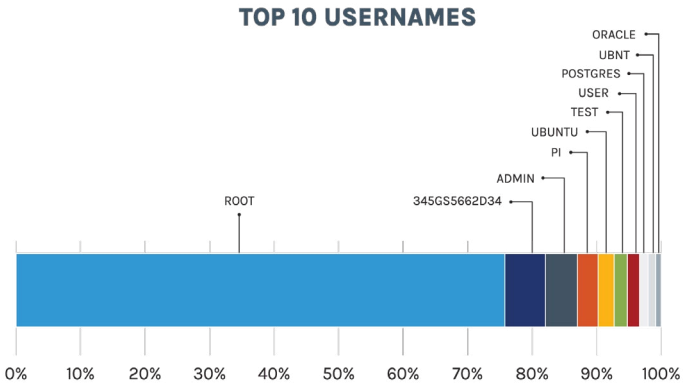
2.4. Weak Credentials – a Return to Generic Usernames



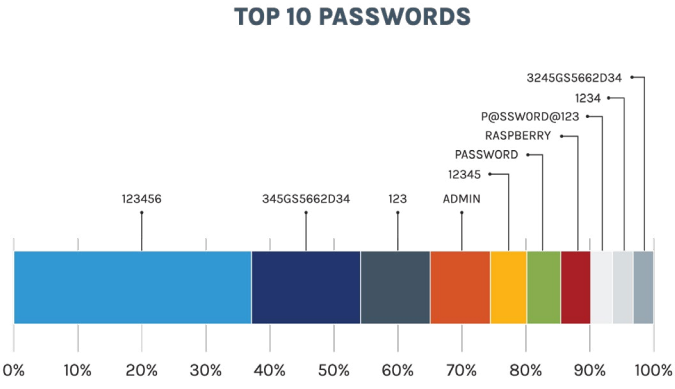
Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

Figure 4 – Top abused credentials

Figure 4 shows the most abused credentials we observed, divided in two categories:

Generic usernames include “root,” “admin,” “user,” “guest” and several other such credentials. The increase from 85% in 2023 to 95% in 2024 shows that attackers are again relying more heavily on brute-forcing and simple dictionary attacks than on targeting specific devices. This is even higher than the 87% we observed in 2022. Specific usernames (decreased from 15% to 5%) can be associated to specific roles, such as “www,” “backup,” “deployer” or even specific applications and devices, such as “odoo,” “rpi,” “kafka,” “zabbix” or “ec2-user”

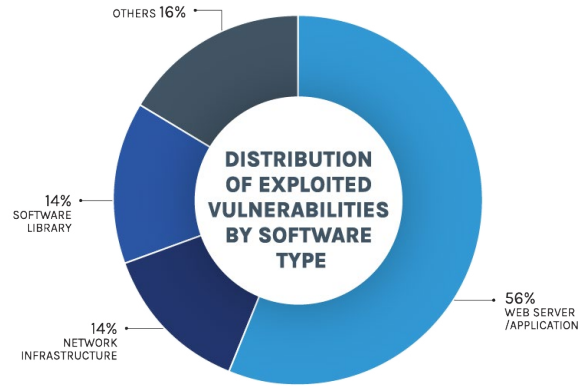
Even though the overall percentage of specific usernames decreased, it’s still relevant to analyze the breakdown of types of specific usernames that attackers are abusing. In 2023, the most popular category was IoT devices (35%), which is now the fourth most abused type of username. Database, DevOps and Cloud all became much more relevant than in previous years. The data is consistent with what we discussed in section 2.3, since often these types of services are web applications.

In the IoT category, the most popular usernames were “ubnt” (for Ubiquiti routers), “moxa” (for industrial networking) and “zyfwp” (for Zyxel firewalls). In February 2024, we published an analysis of botnets targeting Ubiquiti routers since there was a takedown of Moobot which had been commandeered by Russia’s APT28.

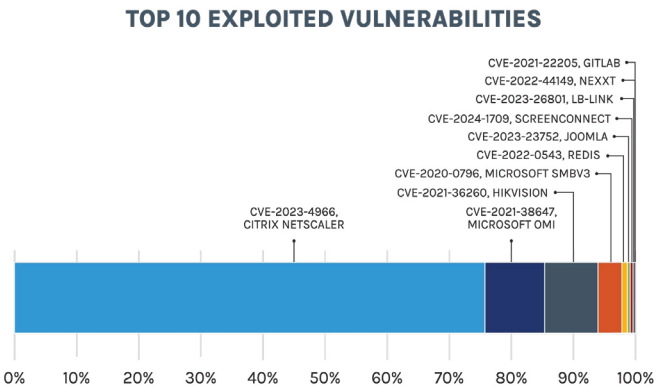
Fact: Best practices for credential management are crucial to prevent attacks leveraging weak credentials.

Insight for Defenders: NIST released an updated version of its digital identity guidelines in August 2024 that challenges some long-held assumptions in the cybersecurity community about password complexity and the need for periodic changes.

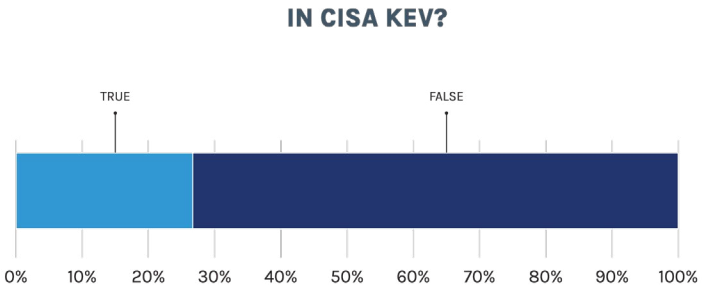
2.5. Exploits – There's Still Much Beyond KEV



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

Figure 5 – Vulnerabilities exploited during the study period

Exploit attempts against web servers and applications have been on a steady rise since 2022, and continue as the largest category we see:

- 2022: 14%
- 2023: 36%
- 2024: 56%

This is in line with what we observed for targeted services in section 2.3.

Exploits against network infrastructure devices, such as firewalls, routers, and VPN appliances increased from 3% in 2022 to 11% in 2023 and now 14%, becoming the second most popular category. We discussed this ongoing trend in our 2024H1 threat review. Software libraries continue to decrease as a percentage of targets for exploitation:

- 2022: 76%
- 2023: 29%
- 2024: 14%

Several categories of IoT devices and other applications known to be often exposed and vulnerable are also routinely targeted, but this category decreased from 24% to 16%.

Three other observations are relevant: Five of the top 10 most exploited vulnerabilities we reported in 2023 remained in the list in 2024:

- CVE-2021-36260 affecting Hikvision
- CVE-2022-0543 affecting Redis
- CVE-2021-38647 affecting Microsoft Windows
- CVE-2020-0796 affecting Microsoft Windows
- CVE-2021-22205 affecting GitLab

Two new entries are especially relevant: CVE-2023-4966 and CVE-2024-1709. CVE-2023-4966 which affects Citrix NetScaler appeared as a 0-day in 2023 but continued to be heavily exploited in 2024. CVE-2024-1709, affecting ConnectWise ScreenConnect, is notoriously easy to exploit and was used in ransomware campaigns. Only one of these has been on the list since 2022: CVE-2022-0543 which affects Redis on Debian systems.

The percentage of exploited vulnerabilities not in CISA's Known Exploited Vulnerabilities (KEV) increased from 65% to 73%. We published a study in May detailing this phenomenon and predicting that it would continue to increase as attackers explore more of organizations' attack surface beyond traditional endpoints.

When we merge our AEE data with observations from the Shadowserver foundation, we come up with a list of at least 25 vulnerabilities affecting OT and Industrial IoT devices that are exploited by botnets or automated attacks and which are not included in CISA's KEV (shown below).

Vendor	Products	CVEs
Apsystems	Altenergy Power Control Software	CVE-2023-28343
Carel	pCOWeb	CVE-2019-11370
CHIYU Technology	CHIYU BF-430, BF-431 and BF-450M	CVE-2021-31250
CONTEC	SolarView Compact	CVE-2023-23333 CVE-2022-29303 CVE-2022-40881 CVE-2023-29919
Eaton	Intelligent Power Manager	CVE-2018-12031
ECOA	Building Automation System	CVE-2021-41293
Emerson	Dixell XWEB-500	CVE-2021-45420
Endress+Hauser	WirelessHART Fieldgate SWG70	CVE-2018-16059
frangoteam	FUXA	CVE-2023-33831
Honeywell	Honeywell PM43	CVE-2023-3710
KevinLAB	Building Energy Management System	CVE-2021-37291
Linear	eMerge	CVE-2019-7254 CVE-2019-7256 CVE-2022-46381
Loytec	LGATE-902	CVE-2018-14918
Open Automation Software	OAS Platform	CVE-2022-26833
Schneider Electric	EVlink City, Parking and Smart Wallbox	CVE-2021-22707
Schneider Electric	SpaceLogic C-Bus Home Controller	CVE-2022-34753
Teltonika	Teltonika RUT9XX series	CVE-2018-17532
Viessman	Vitogate 300 BN/MB	CVE-2023-45852
WAGO	WAGO products (multiple)	CVE-2023-1698
ZKTeco	ZKTeco ZEM500-510-560-760, ZEM600-800, ZEM720, ZMM	CVE-2022-42953

Guidance: Pay more attention to attacker goals and industry targets over country of origin alone.

Insight for defenders: Blocking communications simply by country of origin is not effective. Similarly, knowing where threat actors come from is not necessarily the most useful information. However, knowing what their goals are and what industries they are attacking can help to prioritize strategic security investments. Organizations in the most affected industries, especially, should pay attention to the latest threat intelligence to monitor campaigns that target specific sectors.

2.6. OT Attacks – Increased Focus on Building Automation

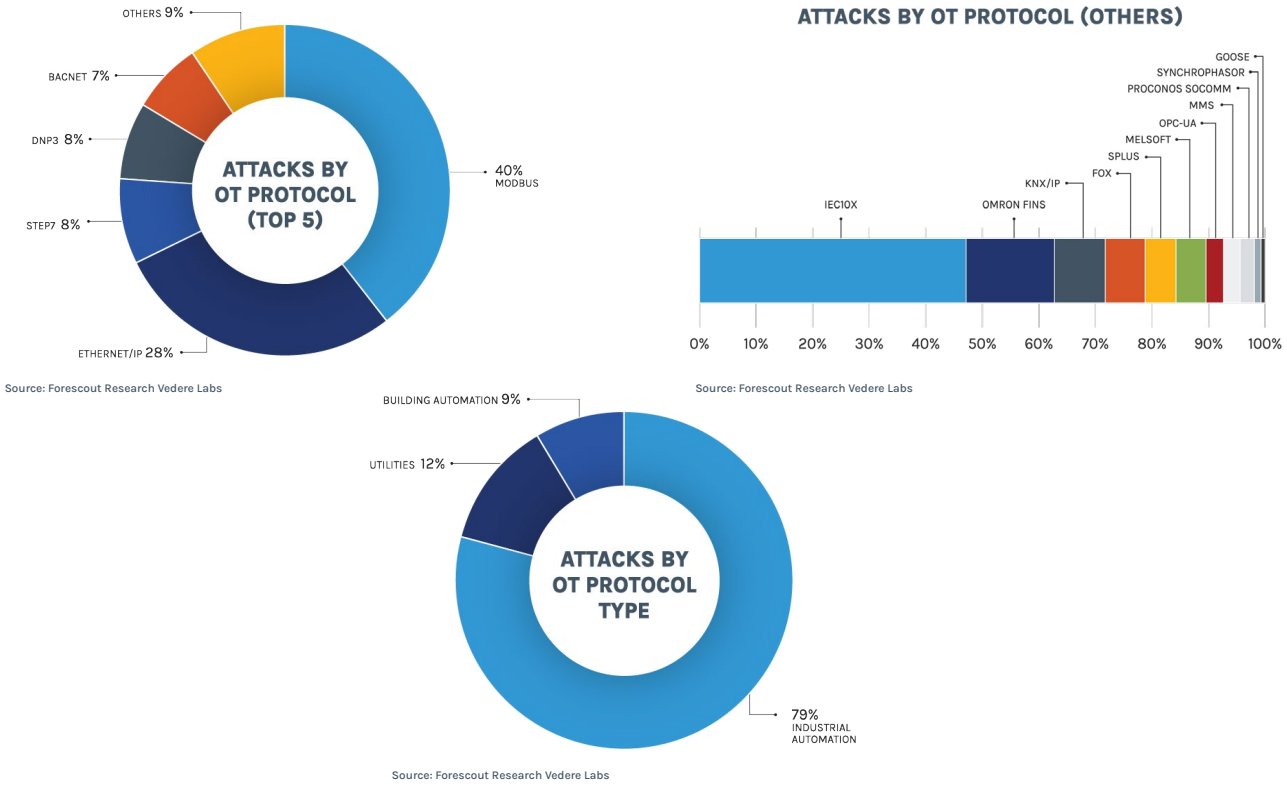


Figure 6 – Attacks against OT protocols

Figure 6 shows the distribution of attacks targeting OT protocols. As in 2023, we highlight five protocols as the top exploited:

1. Modbus, the most popular and most often exposed, OT protocol increased from 33% to 40%
2. EtherNet/IP increased from19% to 28%
3. Step7, used by Siemens devices, decreased from 18% to 8%
4. DNP3, often used in utilities, decreased from 18% to 8%
5. BACnet, used for building automation, is the fifth most attacked protocol with 7% of total attacks

The list of other protocols remained similar to last year — with two notable changes. ‘Others’ increased from 2% to 9% and a new building automation protocol (KNX/IP) appeared on the list as the third most relevant. Overall, the data paints a picture of a heavy interest in Modbus and more fragmented interest in a diversity of other protocols. It means it is not enough to focus on the ‘popular’ protocols for which the most common attack tools are available.

Looking at categories, we see that attacks on industrial automation protocols increased from 71% to 79%, utilities decreased significantly from 28% to 12% and building automation increased from 1% to 9%. The most relevant increase is in the building automation category — especially when we look at the new protocols being attacked. Last year, we discussed how attacks on building automation focused on exploiting vulnerabilities rather than interacting directly with protocols. This year, we see that the interest in building automation protocols is increasing as attackers are still exploiting vulnerabilities on those devices (as evidenced by the table in section 2.5).

Fact: Monitoring the traffic to and from OT devices is now as critical as monitoring IT traffic.

Insight for defenders: Attackers are constantly probing OT/ICS assets for weaknesses. Many organizations will be blind to them because they do not have visibility into their OT/IoT infrastructure. The truth is that building automation, and protocols such as Modbus, are now found in almost every organization and are a target for attackers.

2.7. Attacker Actions/TTPs – the Rise of Discovery

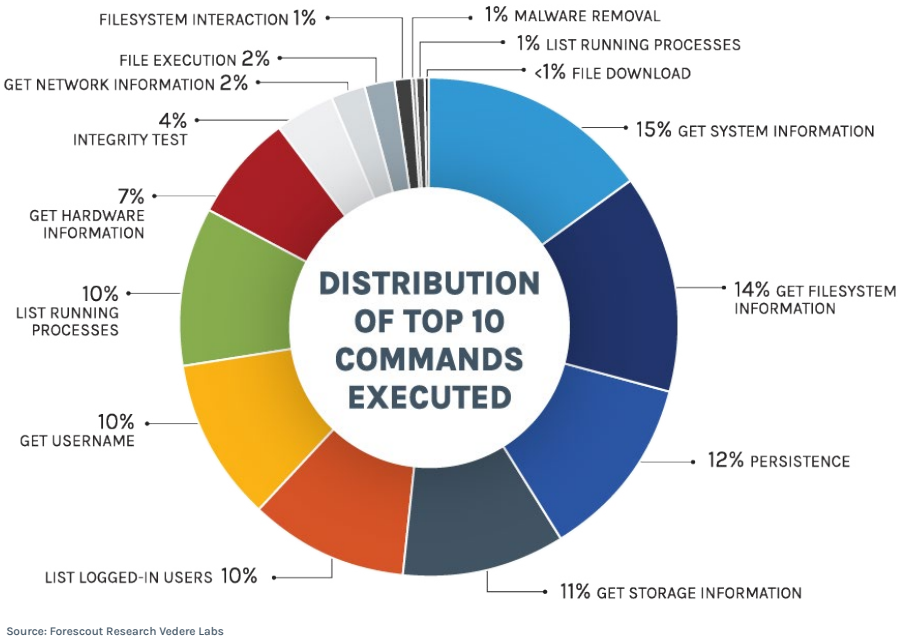


Figure 7 – Top executed commands

Figure 7 shows the distribution of top 10 commands executed after attackers managed to get initial access — mainly over SSH or Telnet. Most of the attacks we observed were automated and used the following ATT&CK tactics:

TA0007 – Discovery represents around 84% of post-exploitation activities, up from 25% in 2023.
These activities include obtaining information such as CPU, RAM, filesystem, operating system and architecture, as well as listing logged-in users, running processes and scheduled jobs. Discovery accounted for 95% of actions in 2022.

TA0003 – Persistence represents around 12% of observed commands, down from 50% observed in 2023 but still up from the original 3% in 2022.
Persistence comprises four main procedures: persisting SSH keys, downloading backdoored shells, creating or manipulating user accounts and executing background processes.

TA0002 – Execution represents around 4% of observed commands, down from 25% in 2023 but also still up from the 1% of 2022.
These commands are related to interacting with the filesystem, downloading and executing further malware.

Fact: An increase in discovery actions means attackers are spending more time interacting with a breached system before moving on to other targets to either understand the system or to find other potential victims.

Insight for Defenders: More time spent on discovery creates new opportunities for detection before more damaging actions are taken on a device, such as data exfiltration, deletion or encryption. It is crucial to be able to detect signs of these discovery actions as soon as possible, either via endpoint telemetry about system discovery or via network signals generated by network discovery actions.

2.8. Malware – Botnets Again at the Top

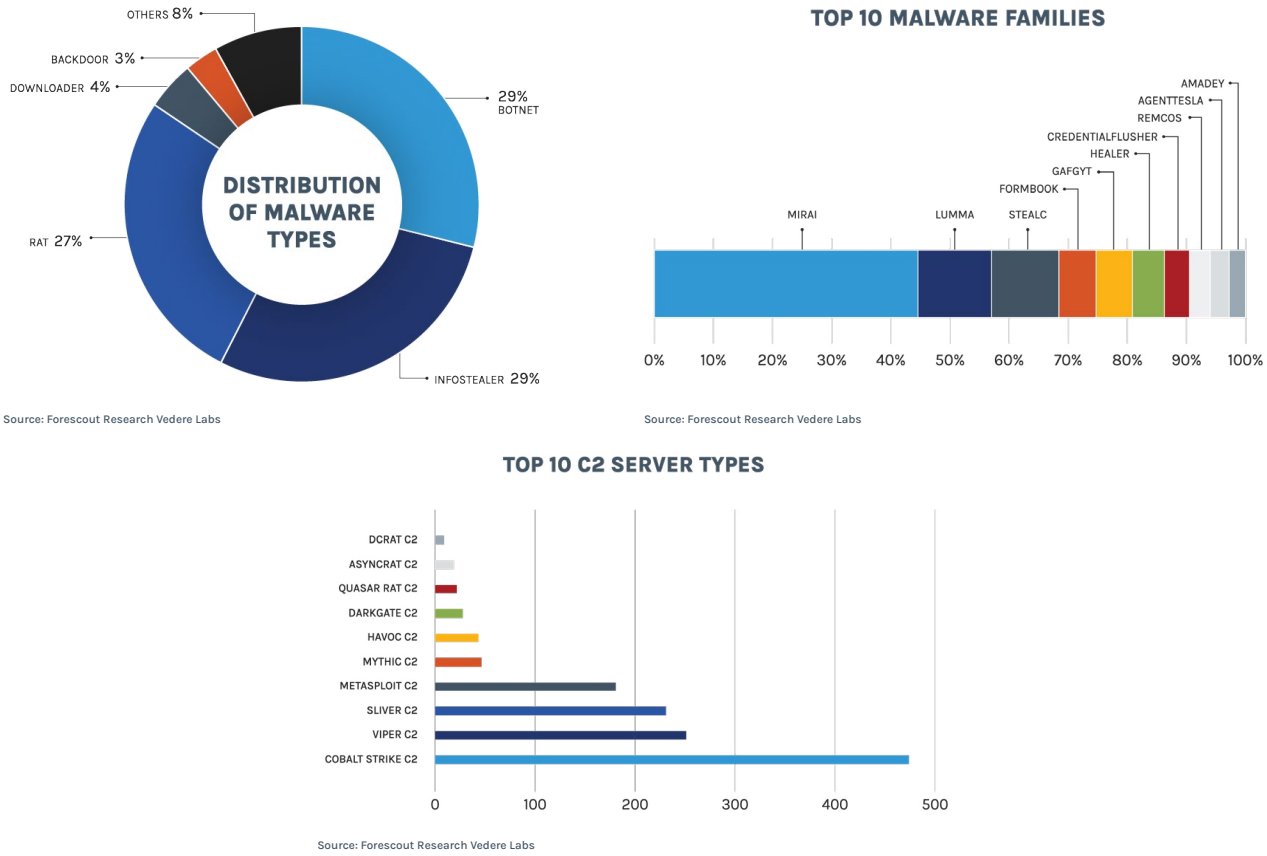


Figure 8 – Distribution of observed malware samples and C2 servers

Figure 8 shows the distribution of malware and observed command and control (C2) servers in our dataset. In 2023, we saw a tie between remote access Trojans (RATs) and information stealers (infostealers) with botnets coming in third place. This year, we see botnets at the top, followed by infostealers and RATs. The 'Others' category includes keyloggers, cryptominers, ransomware, worms and other malicious software. Overall, this data does not show any big changes in the landscape of malware types.

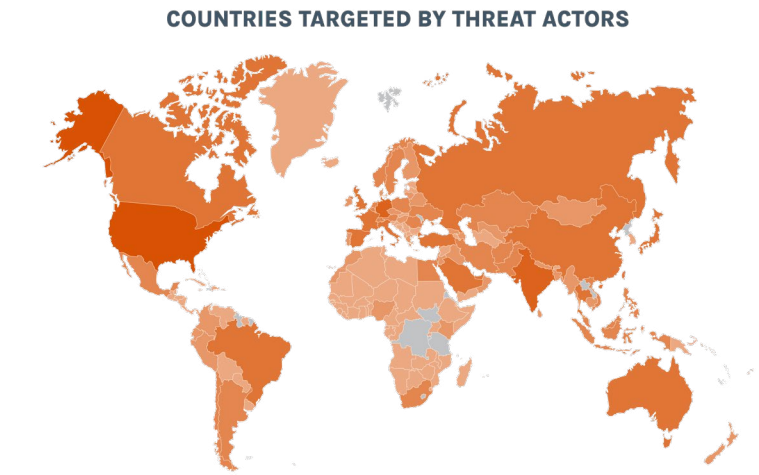
This is different for individual malware families and C2s:

- 5 of the most popular malware families of 2024 were not in the 2023 list: Lumma, Gafgyt, Healer, Credential Flusher, and Remcos. Mirai returned to the top as the most popular malware we observe, but Lumma (in second place) is the most popular new entry.
- 4 of the most popular C2 of 2024 were not in the 2023 list: Viper, DarkGate, Quasar, DcRAT. Although Cobalt Strike remains by far the most popular C2, the use of Viper has surged, surpassing even Sliver, which was gaining a lot of attention in 2023.

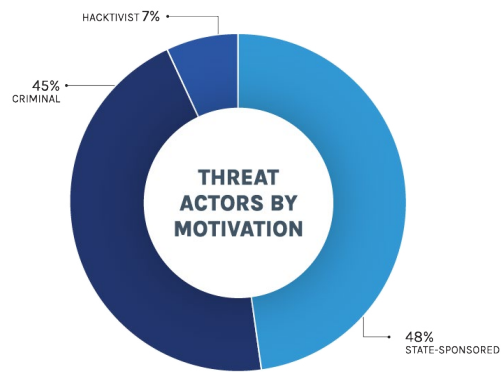
Fact: Although individual malware samples and families evolve every day, the basic nature of malware remains unchanged.

Insight for defenders: The combination of RATs, botnets, infostealers and C2 servers is by now well-known to attackers and defenders. As always, this means it is much more productive for defenders to detect and hunt for TTPs and anomalous behavior than to rely solely on file hashes and C2 IPs which change constantly.

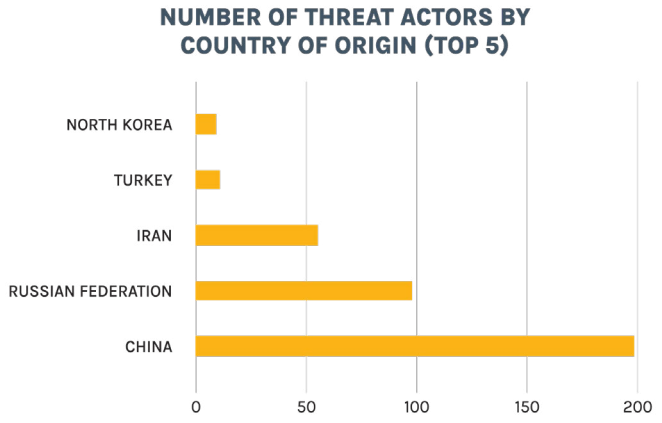
2.9. Threat Actors – More Conflicts Bring More Threat Actors to the Scene



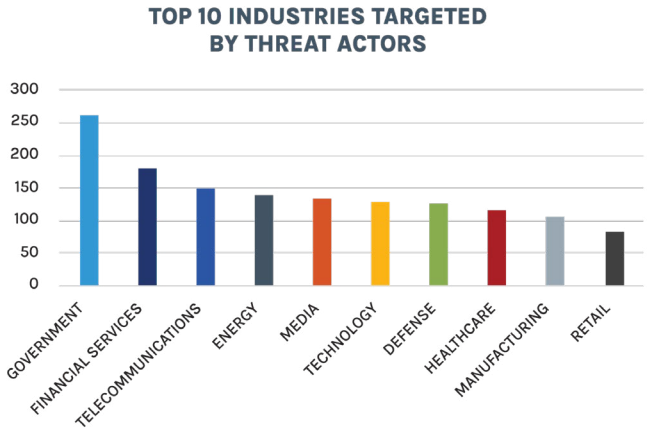
Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

Figure 9 – Distribution of threat actors

We maintain a database of more than 800 threat actors, an increase of 33% with respect to 2023. This list includes:

- Cybercriminals: 45%, a decrease from 47% in 2023
- State-sponsored actors: 48%, an increase from 46% in 2023
- Hacktivists: 7%, the same as in 2023.

The increase in state-sponsored actors is a reflection of the increasing number and complexity of geopolitical conflicts. One trend we discussed in our 2024H1 threat review is that groups previously classified as hacktivist have actually been discovered to be disguised state-sponsored actors, taking advantage of the publicity and plausible deniability offered by hacktivism.

Another relevant trend is the use of cybercriminal infrastructure, such as botnets, by state-sponsored actors, who previously relied on their own infrastructure. This happens mainly via the use of common botnets. Two events

we analyzed in 2024 highlight this trend: The attacks on Denmark's power sector and the Moobot takedown. Additionally, state-sponsored actors are increasingly purchasing access from initial access brokers (see thediscussion in section 2.2)

Figure 9 shows how these actors were distributed in 2024 in terms of origins and targets:

- Threat actors have targeted 176 countries
  - 13 more than in 2023
  - Based in over 40 countries
- The U.S. is the most targeted by 264 actors
- Germany is second: 144
- India is third: 141
- Most threat actors originated from:
  - China: 199
  - Russia: 98
  - Iran: 55
  - These 3 countries account for 43% of threat actor groups
- Government, financial services and telecommunications are the most targeted industries
- The main change is the rise of attacks on telecommunication organizations
- For example, the Salt Typhoon attacks revealed in September
  - The threat actor targeted major ISPs and is well-positioned for:
    - Espionage
    - Disruption activities

Guidance: Pay more attention to attacker goals and industry targets over country of origin alone.

Insight for defenders: Blocking communications simply by country of origin is not effective. Similarly, knowing where threat actors come from is not necessarily the most useful information. However, knowing what their goals are and what industries they are attacking can help to prioritize strategic security investments. Organizations in the most affected industries, especially, should pay attention to the latest threat intelligence to monitor campaigns that target specific sectors.

3. Evolution of Attacks on Critical Infrastructure

Looking at the industries most targeted by threat actors in section 2.9, it's clear that these actors prefer critical infrastructure (CI) sectors. In this section, we deep dive into attacks on these sectors from two points of view:

- **Who is being attacked?**
- **Who is attacking critical infrastructure?**

3.1. Who Is Being Attacked?

To understand which CI sectors are being attacked every year, we complement our Threat Actor Knowledgebase with incident data from the European Repository of Cyber Incidents (EuRepoC), an independent research consortium that provides scientific analysis of cyber incidents. We only take incidents added to the database until December 12 each year to have the same date up to 2024.

Figure 10 shows the total number of incidents and the number of incidents targeting CI sectors in the EuRepoC database per year. It is clear that both the total number of incidents and those affecting CI are increasing, as shown by the trendlines. The total number of incidents increased by 12% from 2023 to 2024 and the number of CI incidents increased by 10% in the same period. The most interesting is that the proportion of incidents on CI changed drastically between 2022, when it was 34%, and 2023, when it became 58%. This proportion remained similar in 2024 (57%).

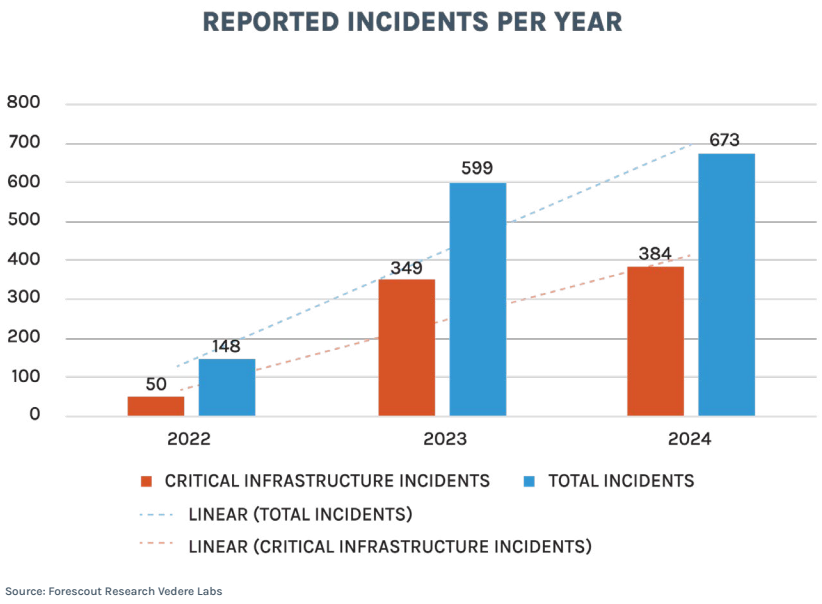
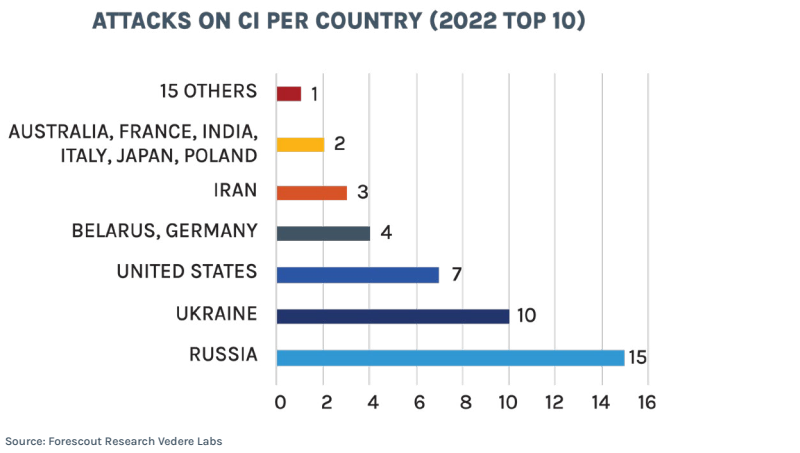


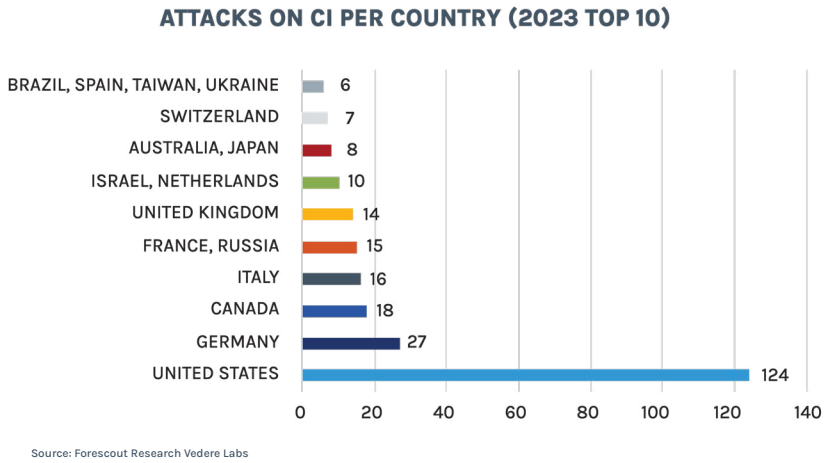
Figure 10 – Incidents per year on the EuRepoC database

The countries with most incidents per year are shown in Figure 11. Three data points stand out:

1. In 2022, Russia and Ukraine topped the list because it was the hottest phase of their ongoing conflict.
2. In 2023 and 2024, the United States experienced the most incidents by far.
3. Overall, CI incidents are becoming more globally distributed across Europe (Germany, France, Spain, Italy, UK) and Asia (Japan, India, Korea, Taiwan, Singapore).

Between 2022 and 2024, there has been a 192% increase in the number of countries experiencing CI incidents. In 2022, CI incidents affected only 27 countries. In 2023, 57 countries. In 2024, it is 79 countries.





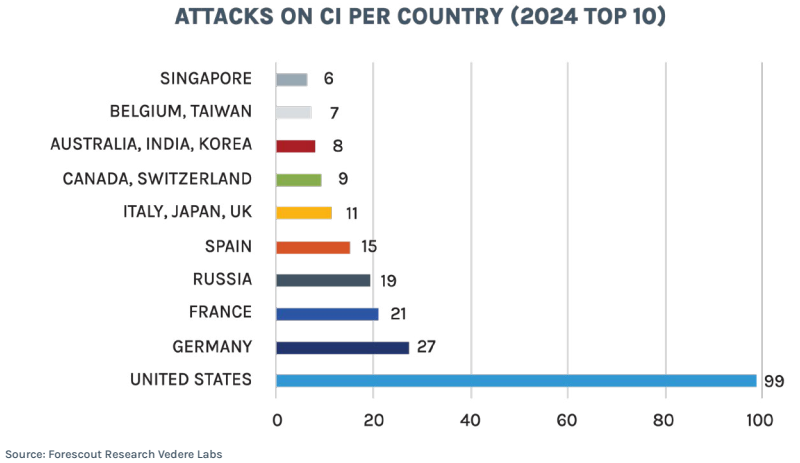
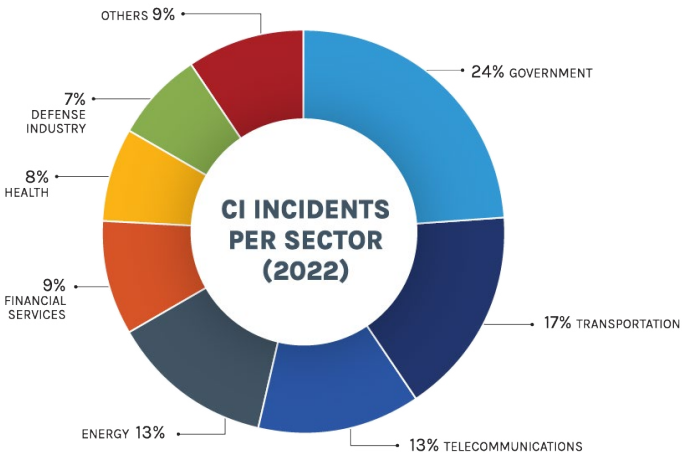
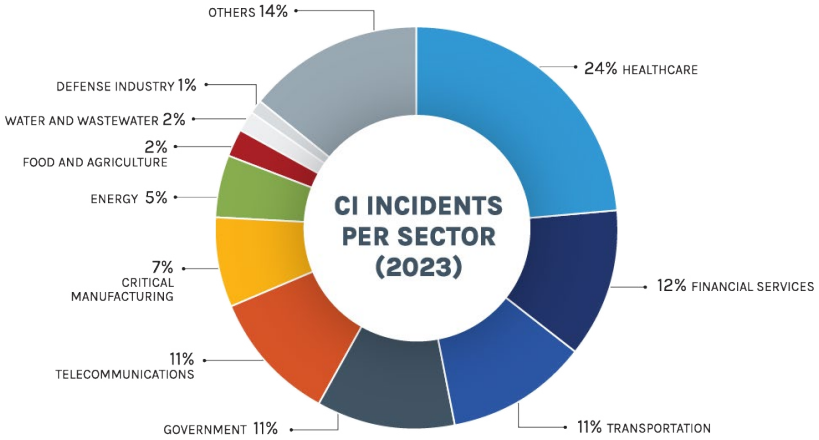


Figure 11 – CI incidents per country

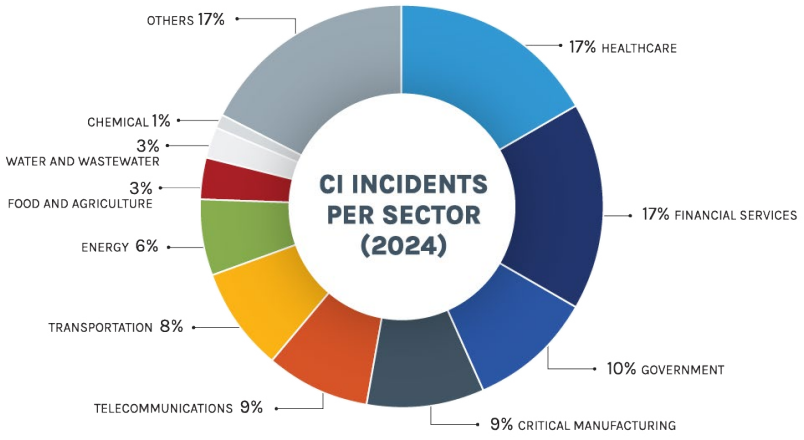
Figure 12 shows the CI sector with most incidents globally per year. Since different countries consider different sectors to be part of critical infrastructure and call them differently, we decided to adopt CISA's definitions and highlight those sectors considered critical in the US (the country with the highest number of incidents). Healthcare was the sector with most incidents both in 2023 and 2024, although the percentage decreased from 24% to 17%. Financial services was also top 2 in both years but saw a relative increase from 12% to 17%. Government jumped from fourth place in 2023 to third in 2024 while manufacturing jumped from sixth to fourth.



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

Figure 12 – CI incidents per sector

3.2. Who Is Attacking?

Taking into account the number of threat actors targeting each CI sector (section 2.9) and the number of incidents in each CI sector (3.2) we drill down into the threat actors targeting five of the most relevant in 2024: Healthcare, financial services, government, manufacturing and energy.

The following Figure 13 summarizes the actors targeting each sector. Here is what stands out:

1. **The majority of threat actors are cyber-criminals in healthcare, financial services and manufacturing.** This is partly because attacking those sectors can be very lucrative. The value of data when exfiltrated or because those organizations prefer to pay threat actors rather than wait for long recovery actions while production/business is down.

2. **The majority of threat actors are state sponsored in government and energy.** That is partly because these sectors are highly relevant for espionage, pre-positioning activities in case of future conflicts or potential for physical disruption in ongoing conflicts.

3. **Hacktivist activity is more common in the government sector** which coincides with the fact that hacktivist attacks nowadays align with geopolitical motivations.

4. **Threat actors from China, Russia, Iran and North Korea appear in every CI sector of the top 5.** Brazil also hosts a large number of actors targeting financial services, manufacturing and energy.

5. **The number of threat actors between 2023 and 2024 has increased the most in energy (93%), manufacturing (71%) and healthcare (55%).**

6. **Spearphishing Link (T1566.002) is still the preferred initial access technique for threat actors across most CI sectors** — even with the rise of exploits of public-facing applications and devices.

7. System Owner/User Discovery (T1033) is the favorite discovery technique.

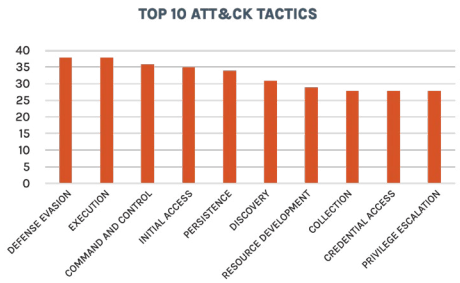
8. Scheduled Task (T1053.005) is the preferred execution method.

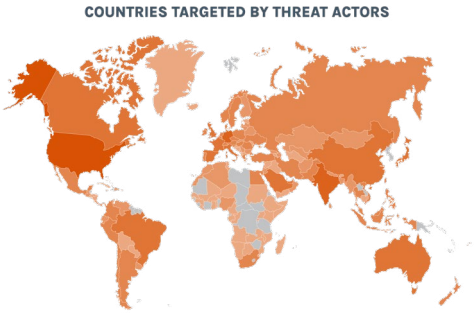
Healthcare

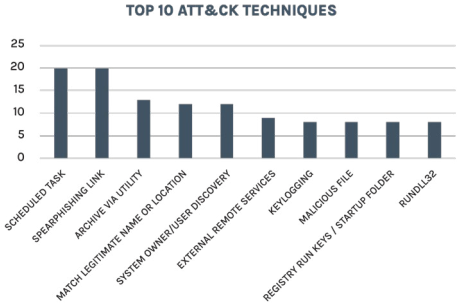
Total number of threat actors:

115

(+55% from 2023)



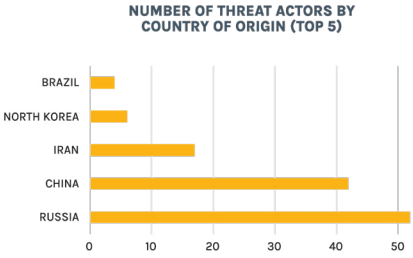


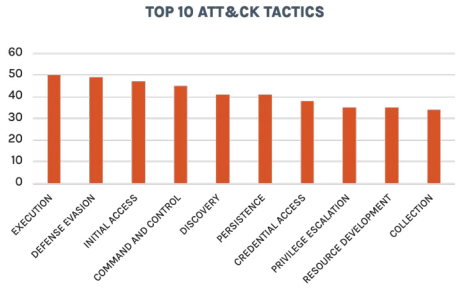


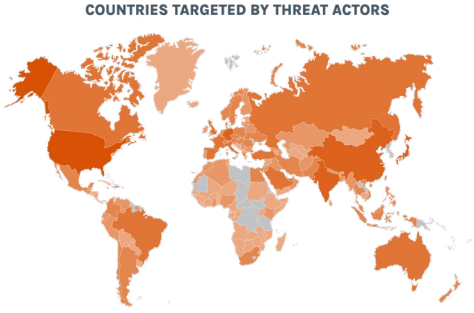
Financial Services

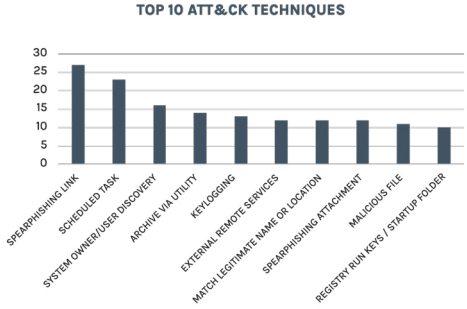
Total number of threat actors:

181







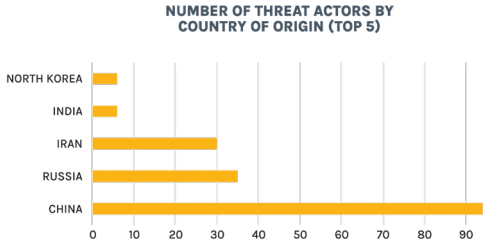


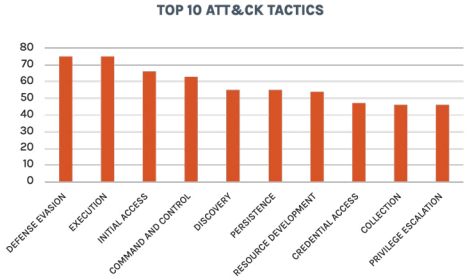
Source: Forescout Research Vedere Labs

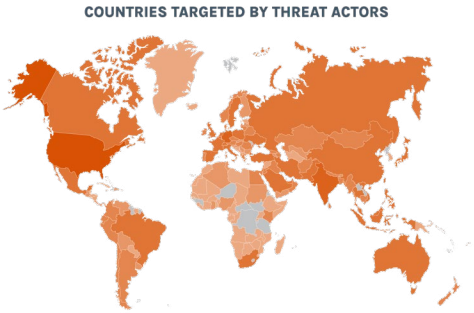
Government

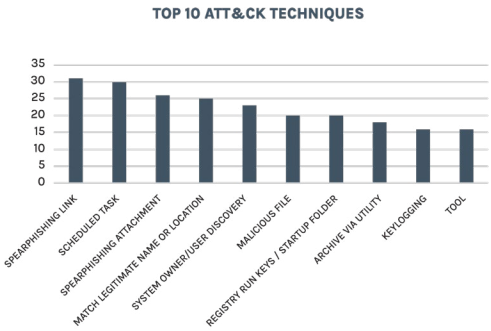
Total number of threat actors:

262





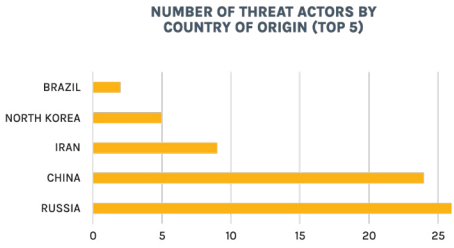


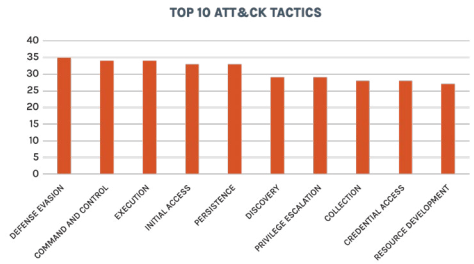


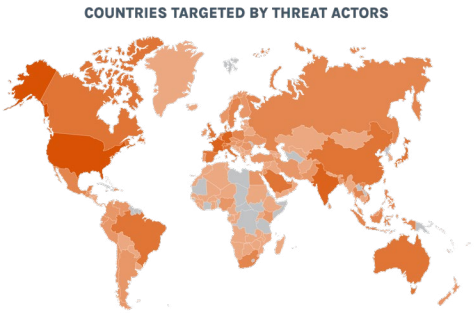
Manufacturing

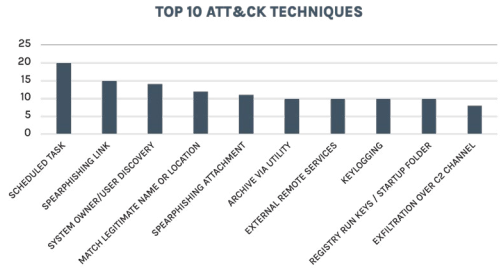
Total number of threat actors:

108







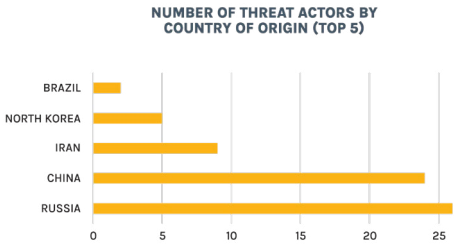


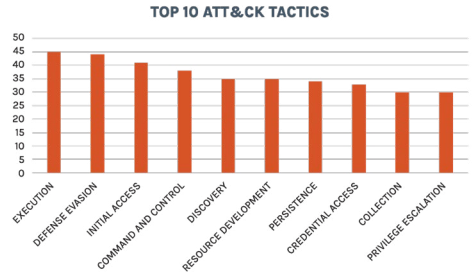
Source: Forescout Research Vedere Labs

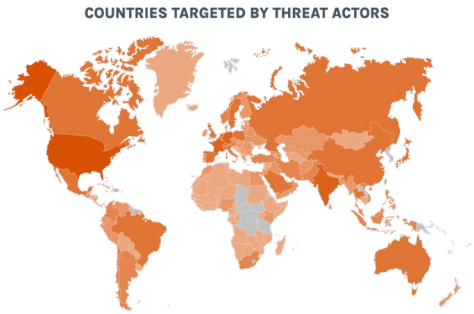
Energy

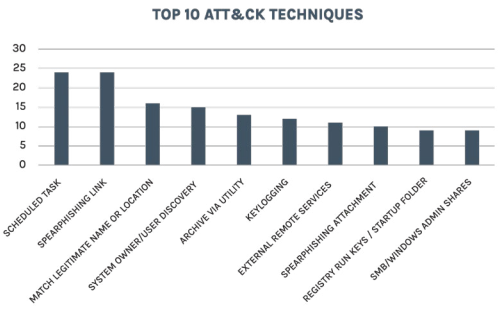
Total number of threat actors:

139









Source: Forescout Research Vedere Labs

Figure 13 – Vertical industry data

4. Conclusion

In this report, we analyzed data relating to the attacks, exploits, malware, and threat actors we observed in 2024. Throughout this report, we included insights for defenders alongside each of the main findings. We recommend organizations focus on three key pillars of cybersecurity at a more strategic level:

- **Risk & Exposure Management.** Start by identifying every asset connected to the network, its criticality, credentials, open ports and general security posture.

  Change any default credentials and use strong, unique passwords for each device. Next, unused services should be disabled and vulnerabilities patched to prevent exploitation. Finally, focus on risk mitigation using automated controls that do not rely only on security agents and apply to the whole enterprise, instead of silos like specific IT networks, OT networks, or specific device types.

- **Network Security.** Do not expose unmanaged devices directly to the internet. Segment networks to isolate IT, IoT and OT devices, limiting network connections to only specifically allowed management and engineering workstations, or among unmanaged devices that need to communicate.

  Segmentation should not happen only between IT and OT, but even *within* IT and OT networks to prevent lateral movement and data exfiltration. Restrict external communication paths and isolate or contain vulnerable devices in zones as a mitigating control, if they cannot be patched or until they can be patched.

- **Threat Detection & Response.** Use an IoT/OT-aware, DPI-capable monitoring solution to alert on malicious indicators and behaviors, watching internal systems and communications for known hostile actions such as vulnerability exploitation, password guessing or unauthorized use of OT protocols. Anomalous and malformed traffic should be blocked, or its presence should at least be alerted to network administrators.

  Beyond network monitoring, threat detection and response solutions collect telemetry and logs from a wide range of sources including security tools, applications, infrastructure, cloud and other enrichment sources, to correlate attack signals, generate high-fidelity threats for analyst investigation and provide the ability to automate response actions across the enterprise.