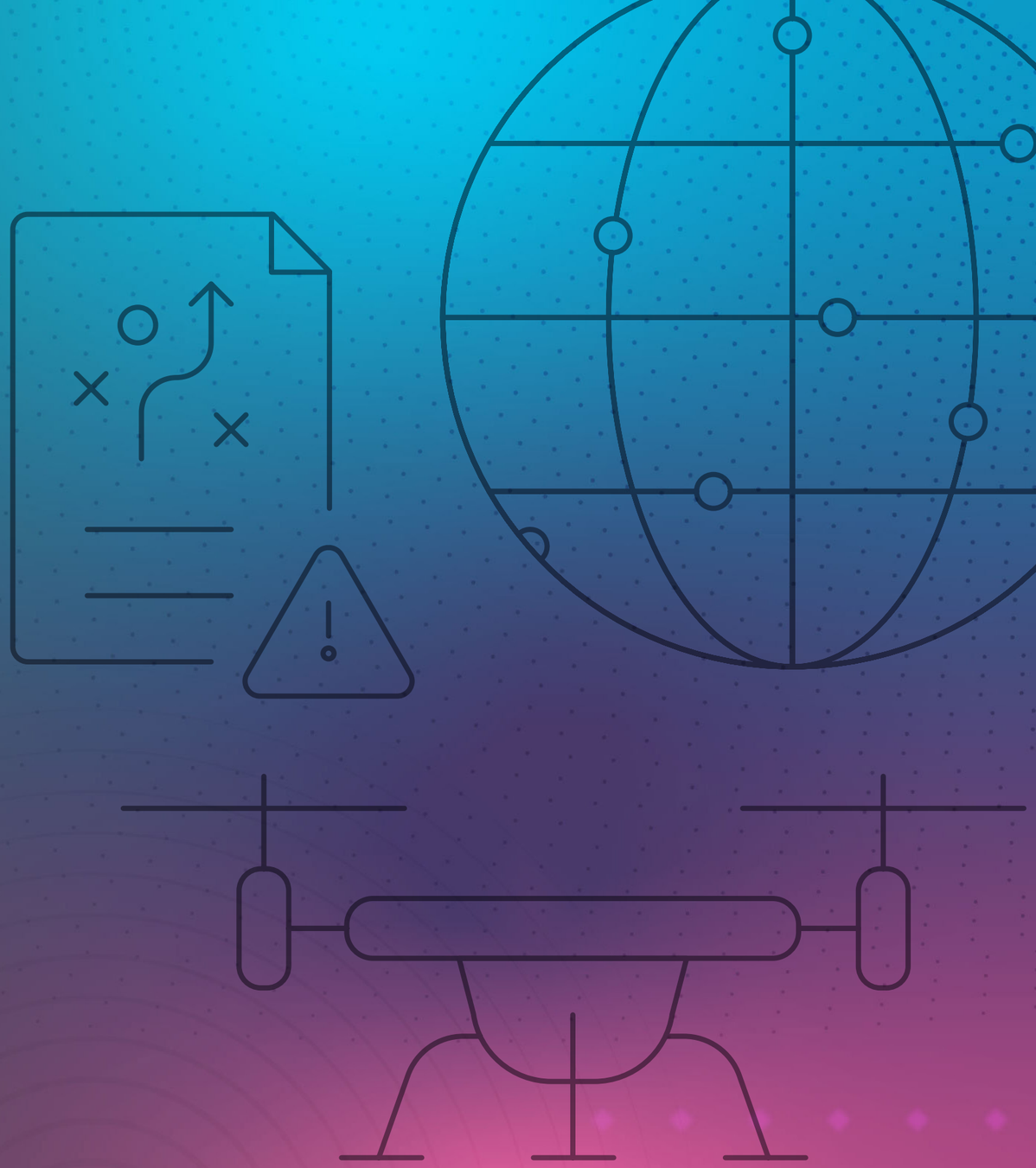
NOZOMI NETWORKS LABS



2025 1H REVIEW

OT/IoT Cybersecurity Trends and Insights

July 2025

About Nozomi Networks Labs

Nozomi Networks Labs is dedicated to reducing cyber risk for the world's industrial and critical infrastructure organizations. Through its cybersecurity research and collaboration with industry and institutions, it helps defend the operational systems that support everyday life.

The Labs team conducts investigations into industrial device vulnerabilities and, through a responsible disclosure process, contributes to the publication of advisories by recognized authorities.

To help the security community with current threats, they publish timely blogs, research papers and free tools.

The **Threat Intelligence** and **Asset Intelligence** services of Nozomi Networks are supplied by ongoing data generated and curated by the Labs team.

To find out more, and subscribe to updates, visit **nozominetworks.com/labs**

Table of Contents

1. Executive Summary

Twice a year the Nozomi Networks Labs team assesses the operational technology (OT) and Internet of Things (IoT) threat landscape to provide insights into how industrial organizations and critical infrastructure operators can protect themselves from active, emerging and advanced threats. This report covers the first half of 2025. Except for IoT botnet activity captured by our honeypots, all data in this report derives from the anonymized telemetry of participating Nozomi Networks customers.

If you're a Nozomi Networks customer, you are covered for the vulnerabilities and threats in this report. Asset intelligence and threat intelligence about them is baked into our platform by Nozomi Networks Labs.

Leveraging a vast network of globally distributed honeypots, wireless monitoring sensors, inbound telemetry, partnerships and other resources, our team uncovers trends, novel attack methods and insights to help you safeguard your environment. Our threat intelligence, enriched by indicators of compromise, threat actor profiles and vulnerability data from Mandiant, empowers customers to proactively defend their systems. By analyzing telemetry informed by this intelligence, our researchers uncover actionable trends and patterns. What follows are highlights from the first half of 2025.

1.1 Key Findings from 1H 2025

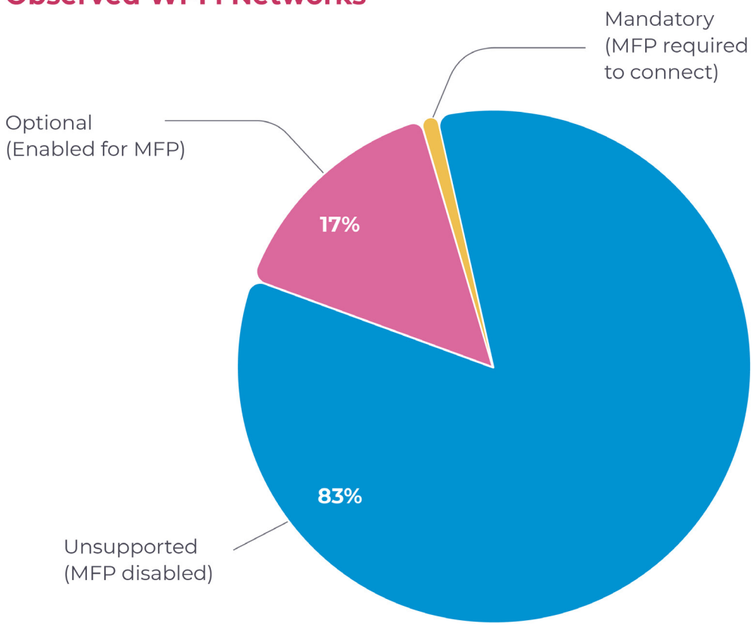
Military Conflicts Spur Increased Cyberthreats

In today's world, global and regional conflicts are always accompanied by increased activity by cyberthreat actors. A year ago, we were analyzing the use of **FrostyGoop (aka BUSTLEBERM)** as a cyber weapon to disrupt critical infrastructure, linked to the ongoing war in Ukraine. In May and June, we observed a **133% increase in cyberattacks** coming from six well-known Iranian threat actor groups, primarily targeting U.S. transportation and manufacturing organizations. These two sectors were also the most targeted sectors globally.

Wireless Networks Remain Wide Open to Attack

Industries increasingly rely on wireless technologies for critical operations, yet the vast majority of Wi-Fi Protected Access 2 (WPA2, the current wireless gold standard) networks are missing basic MFP protection, a critical feature that defends against manipulation of control frames.

802.11w MFP Configuration Status Across Observed Wi-Fi Networks

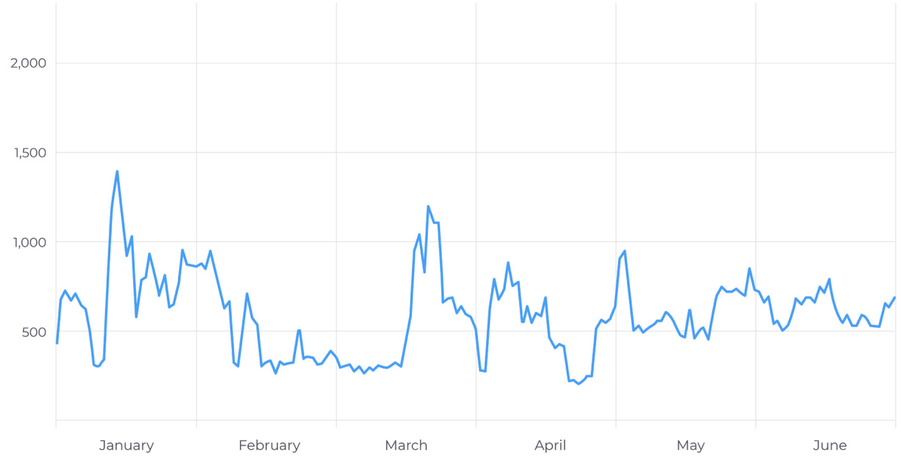


Mirai Variants Are Responsible for IoT Botnet Activity Spikes

Botnet attacks originated predominantly from the U.S, which overtook China in the number of compromised devices. Botnet activity fluctuated daily, with peaks linked to known malware strains such as Mirai. Attackers commonly use default or weak credentials for initial access and target privileged accounts like root and admin.

Daily Volume and Activity from Unique Attacker IP Addresses

January 1 to June 30, 2025



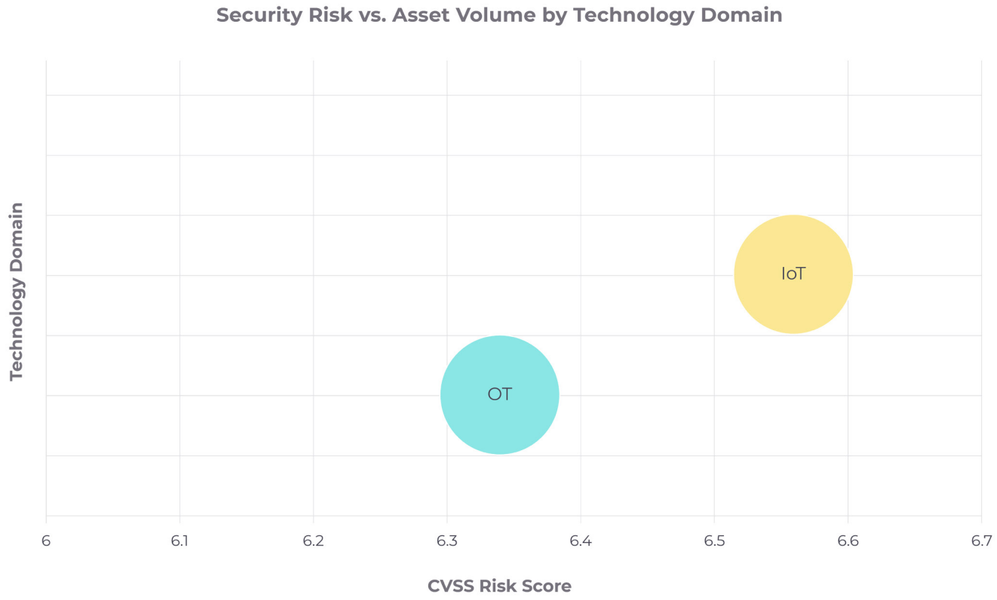
Read on for details about these and other findings, along with insights and recommendations for how to defend critical systems and increase resilience.

2. Introduction

2.1 Diversity of Assets and the Cyber Risk Perspective

In the complex landscape of industrial and critical infrastructure environments, a defining characteristic is the coexistence of three distinct asset domains: IT (Information Technology), IoT (Internet of Things), and OT (Operational Technology). Each of these asset classes brings unique risk profiles, threat surfaces, and operational constraints.

The chart that follows, sourced from Nozomi Networks' extensive telemetry across global deployments, illustrates this asset distribution and highlights a critical insight: while OT assets may not show the highest average base CVSS scores, they often represent a disproportionately high operational risk due to their criticality, limited resilience and the cascading effects their compromise could generate.



Nozomi Networks continuously collects and analyzes fully anonymized telemetry across IT, OT, and IoT environments, enabling an early detection of emerging threats and a data-driven view of evolving risks. This real-world perspective helps anticipate attack vectors before they become widespread, offering defenders the visibility necessary to prioritize defensive efforts in high-value operational areas.

From a cybersecurity standpoint, the asset mix dictates both strategy and urgency. While IT systems typically benefit from mature security programs and patching cycles, OT systems often run outdated firmware, lack encryption or authentication protocols, and are deeply interconnected with physical processes. IoT introduces a mass of high-volume, often poorly secured endpoints that serve as easy entry points and lateral movement bridges.

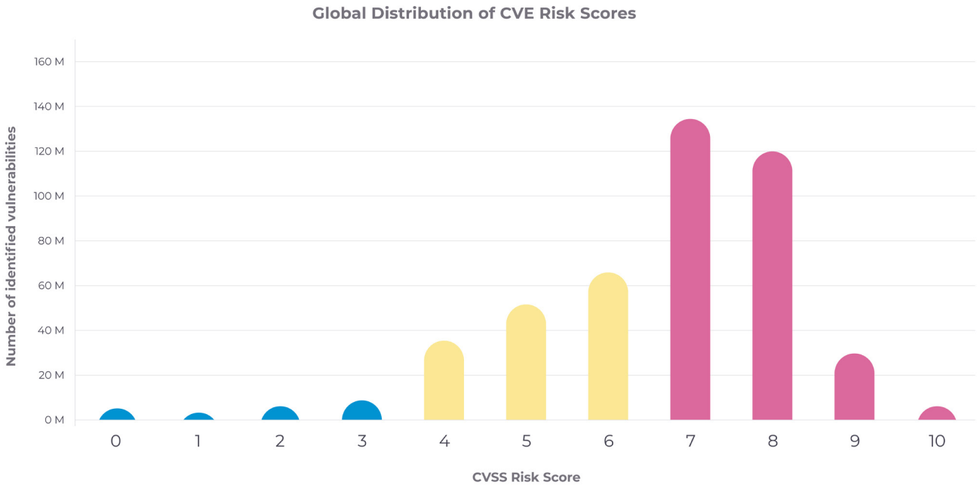
Not all assets are equal and treating them as such undermines risk-based prioritization efforts. Cybersecurity in industrial domains must begin with a clear inventory and contextual understanding of asset types, their operational role, and their exposure, an approach that moves from theoretical threat models to practical risk mitigation.

2.2 Understanding Risk Through a Global Lens

Building on the necessity of risk-based prioritization, a natural question arises: how do we quantify and compare cyber risk in a standardized way, regardless of the technological domain in question? This is where the Common Vulnerability Scoring System (CVSS) becomes a foundational element in cybersecurity risk assessment.

CVSS provides a structured methodology to evaluate the severity of vulnerabilities in a vendor- and asset-neutral fashion. It allows organizations to move from fragmented, asset-specific perceptions of risk toward a unified model that supports prioritization at scale. This is especially crucial in environments that blend IT, OT and IoT, where the temptation to treat each domain in isolation can lead to blind spots and misallocated resources.

The CVSS distribution chart, which aggregates vulnerability data independently of the sector or asset class, reveals an important trend: the vast majority of identified vulnerabilities fall within the medium to high severity range, with a significant concentration between CVSS scores 6.0 and 9.0. This suggests that the global vulnerability landscape remains consistently threatening across domains, even if the operational impact of each vulnerability varies widely depending on context.



This distribution highlights the need for strategic filtering and contextual interpretation. A high CVSS score may not always translate into critical operational risk, and conversely, seemingly moderate vulnerabilities can pose serious consequences in sensitive or exposed systems.

Therefore, CVSS should not be treated as a final answer, but as a critical input for contextual decision-making. This understanding sets the stage for the next layer of risk evaluation: the likelihood that a vulnerability will be actively exploited, and how that probability changes the risk equation entirely.

2.3 Risk vs. Exploitability: Adding Real-World Weight to Risk Scores

Having established the severity distribution of vulnerabilities through CVSS, the next logical step is to assess how these vulnerabilities behave in the real world. Not every vulnerability with a high score is equally likely to be exploited, and this discrepancy often leads to a misalignment between perceived and actual risk.

To address this gap, the Exploit Prediction Scoring System (EPSS) was introduced — a complementary metric that estimates the probability of exploitation for known vulnerabilities. While CVSS measures potential impact, EPSS adds an essential predictive layer: it tells us whether attackers are likely to weaponize a given CVE.

Distribution of CVEs by Exploitability and Severity

Exploitability \ Severity	Low	Medium	High	Critical
Very High (75–100%)	0%	1%	2%	10%
High (50–75%)	0%	0%	1%	9%
Medium (25–50%)	0%	1%	2%	9%
Low (0–25%)	99%	97%	95%	72%

The distribution chart of CVEs by severity (CVSS) and exploitability (EPSS) reveals a nuanced view of real-world threat potential. Even among vulnerabilities rated as critical (CVSS), only a fraction — roughly 10% — fall into the highest EPSS tier (75–100% likelihood of exploitation). For those rated high, only 2% reach this tier, with a similarly low presence across medium and low severity categories.

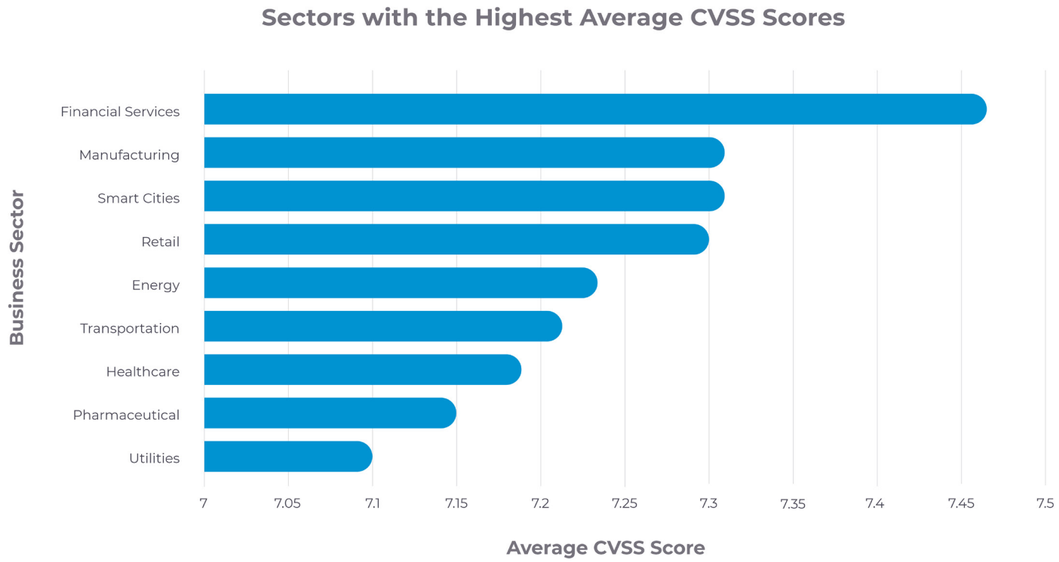
Conversely, most vulnerabilities — over 70% of even critical ones — remain in the lowest EPSS bracket (0–25%), underscoring the fact that not all high-severity issues attract attacker interest or weaponization. This level of granularity is crucial for cyber defenders operating in resource-constrained environments. EPSS empowers teams to go beyond abstract severity and focus on the vulnerabilities most likely to be exploited in active campaigns, significantly improving operational prioritization.

Ultimately, effective cyber defense requires both dimensions: CVSS captures the potential impact, while EPSS quantifies the likelihood of exploitation. Together, they offer a strategic framework that turns theoretical exposure into actionable insight, aligning vulnerability management with current threat realities.

2.4 Sectorial Exposure: Risk Concentration Across Critical Industries

With a clearer understanding of both vulnerability severity and exploitability, it becomes essential to map this risk onto real-world operational contexts. Not all industries face the same level of exposure or threat activity. In fact, attacker interest and the potential impact of compromise vary significantly depending on the sector targeted.

The sectorial distribution chart offers a compelling view and effectively summarizes the most vulnerable sectors across the critical infrastructure spectrum. Unsurprisingly, sectors like Energy, Water & Wastewater, and Transportation rank among the most affected. These verticals are not only central to national stability and continuity of services, but they also tend to rely on legacy systems and highly interconnected operational technologies, often lacking modern cybersecurity controls.



These are, without doubt, the most vulnerable sectors, both in terms of the number of reported CVEs and the persistence of critical security gaps. Across all sectors, the average severity of vulnerabilities remains consistently high, clustering between CVSS scores of 7 and 8. This reinforces the notion that critical infrastructure environments are not only exposed but inherently fragile, with vulnerabilities that, if successfully exploited, can have far-reaching operational and societal consequences.

What stands out is not just the volume of vulnerabilities associated with each sector, but the density of high-risk CVEs that persist within specific domains. For example, industrial energy systems often use proprietary or poorly maintained components that are rarely patched, making them ideal targets for advanced persistent threat actors. Similarly, municipal water systems, while smaller in scope, typically suffer from underinvestment in IT and OT security, making them vulnerable to both automated attacks and targeted campaigns.

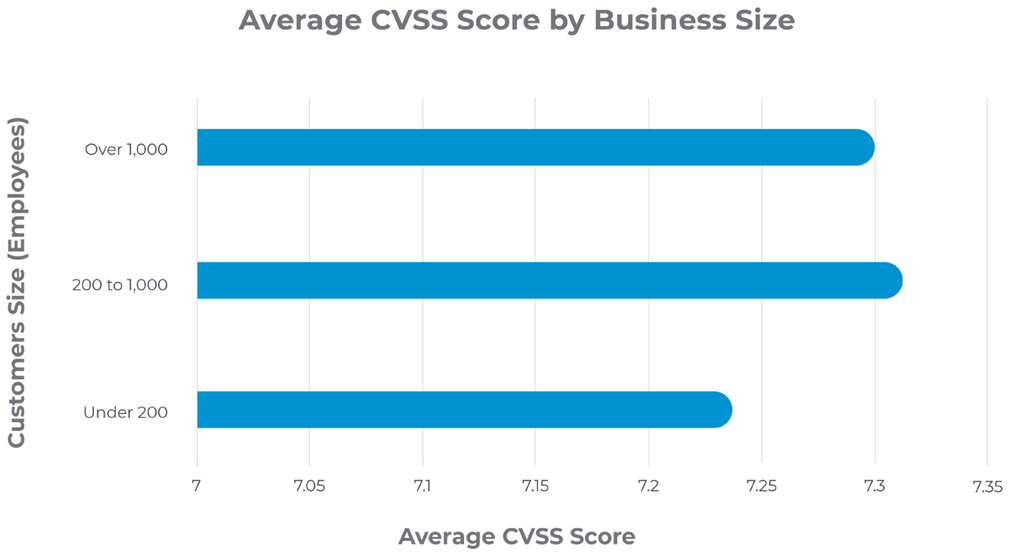
This sectorial lens is invaluable for national cybersecurity strategy and private sector risk planning alike. It provides a threat-centric, rather than asset-centric, view of exposure, one that enables prioritization of controls, sector-specific threat hunting, and tailored detection engineering.

A key takeaway here is the importance of sector-specific threat intelligence. Generic risk scoring is no longer sufficient. Defenders must understand how vulnerabilities map to sectorial realities, and how adversaries are aligning their operations to exploit weaknesses in critical verticals.

2.5 Business Size and Risk Posture: Interpreting Impact at Scale

After analyzing the vulnerability landscape across technological domains and industry sectors, a final layer of context comes from evaluating how business size influences risk posture. The assumption that larger organizations are more secure due to greater resources is often misleading. In reality, attack surface, organizational complexity, and operational interdependencies scale faster than security maturity.

The data presented in the chart illustrates a clear pattern: mid-size and large enterprises bear the brunt of high-risk exposure, particularly within critical infrastructure. These organizations often manage a complex mix of legacy OT, cloud-based IT, and a rapidly growing IoT layer. While they may have more structured cybersecurity programs, their size also makes them more visible, more interconnected, and ultimately, more attractive to adversaries.



At first glance, the variation in average CVSS scores across business sizes may appear modest. However, it is crucial to recognize that we are dealing with statistical averages calculated over an enormous dataset — nearly 500 million vulnerability records. In such contexts, even seemingly small deviations can signal significant shifts in exposure and threat concentration. A difference of just a few decimal points in average severity can translate to a substantial increase in the number of exploitable vulnerabilities with operational impact.

In contrast, smaller organizations tend to have narrower environments, which can reduce exposure but also often lack formalized defense mechanisms, skilled personnel, and response capabilities. As a result, even if they are targeted less frequently, the impact of a successful attack can be disproportionately high.

The key interpretation here is not simply that larger businesses are more vulnerable, but that risk scales non-linearly. A 10x increase in assets does not mean a 10x increase in protection requirements — it often means far more. This applies not only to technical controls but also to cybersecurity budget allocation, staffing, governance, and monitoring capabilities. Without proportional investment and architecture evolution, growth amplifies exposure rather than mitigating it. Moreover, security debt accumulates with organizational growth if visibility and governance are not expanded in tandem.

This data also challenges a purely compliance-driven approach to risk management. In many large enterprises, compliance is decoupled from operational resilience, leaving blind spots that sophisticated adversaries know how to exploit. Ultimately, context-aware, scalable, and intelligence-driven defense strategies are essential to shift from reactive to proactive cybersecurity — regardless of business scale. Defenders should avoid thinking in terms of size alone. Instead, they should evaluate how complexity, exposure, and adversary interest interact to shape the true risk profile of their organization. In this context, adopting purpose-built security solutions for OT and IoT environments is not optional, but fundamental.

Context-aware, scalable, and intelligence-driven defense strategies are essential to shift from reactive to proactive cybersecurity — regardless of business scale.

3. Wireless Threats in Industrial Environments

3.1 The Silent Threats Around Us

In many industrial environments, operators confidently state, "there's no wireless here." The assumption is simple: if everything is cabled, then everything is secure. But wireless communications don't ask for permission. They exist regardless of network architecture, and are constantly happening, in the air, around the facilities, and inside operational systems.

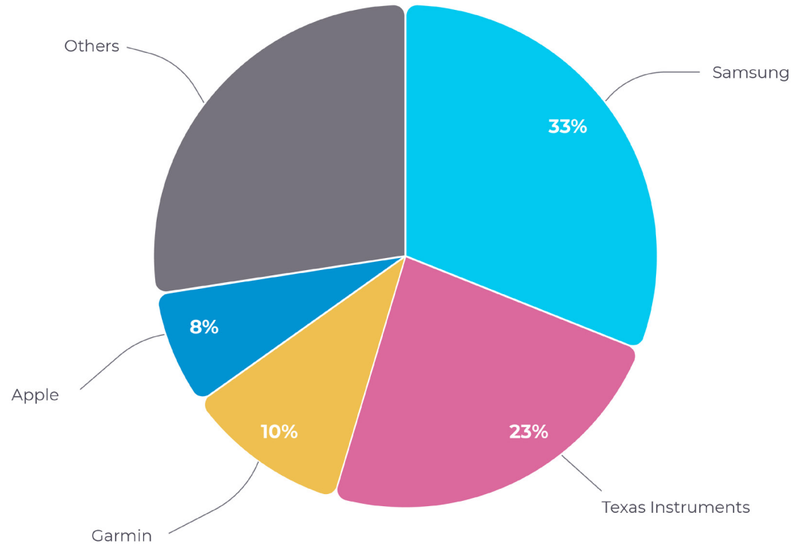
From engineering laptops with Bluetooth enabled to vendor-supplied diagnostic tools to IoT sensors using Zigbee or proprietary 802.15.4 protocols, wireless activity permeates even the most rigorously wired environments. And yet, most organizations have no idea how many devices are actively transmitting around them.

3.2 Ambient Noise: You Are Not Alone

During the first half of the year, our wireless telemetry across monitored environments shows a vast array of consumer and embedded devices operating via Bluetooth. We identified Bluetooth communications from over 50 different device manufacturers across monitored industrial and critical environments.

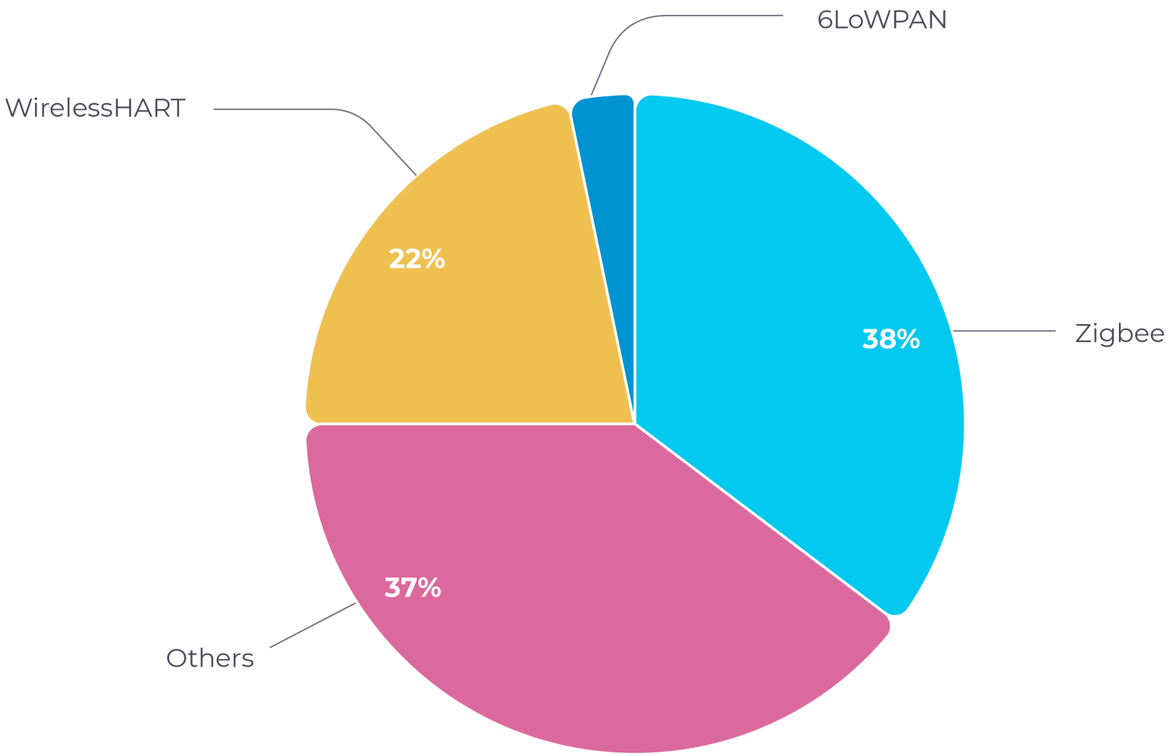
Among these vendors are Samsung, Apple, Bose, Garmin, and Intel — these are not industrial control manufacturers. Their presence suggests BYOD exposure (Bring Your Own Device), technician tools, and even hidden rogue devices. Most of these are not inherently malicious. But they represent an uncontrolled surface that can be exploited or misused without notice. Without visibility into these assets, organizations risk leaving themselves exposed to misconfiguration, data leakage, or unintentional bridging of air-gapped environments.

Vendor Distribution of Bluetooth Assets



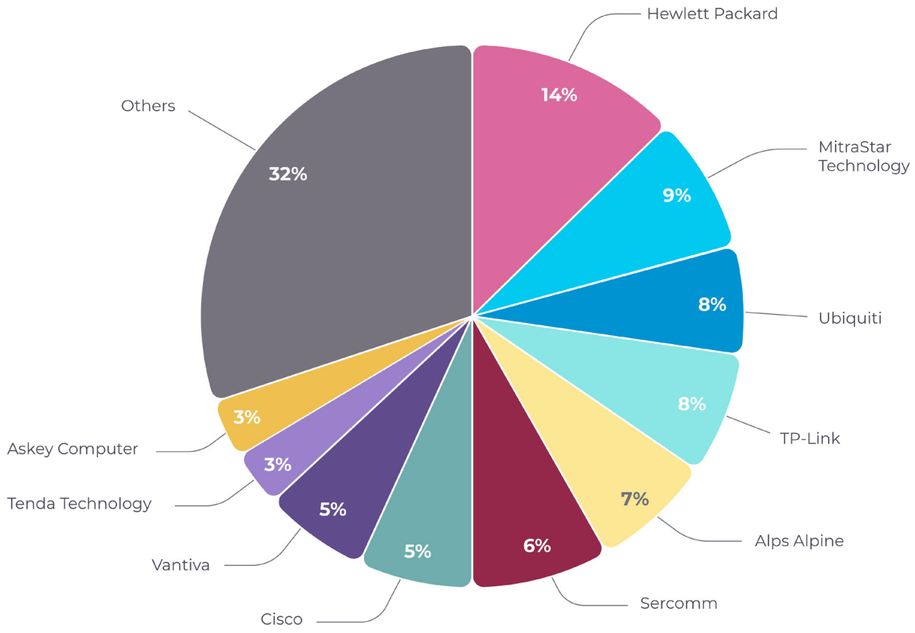
Simultaneously, in the industrial RF spectrum, we see high volumes of low-power protocols. IEEE 802.15.4 networks dominate, including Zigbee and WirelessHART. These protocols are used by field sensors, badge readers, and process automation gear — often with no centralized inventory or security oversight. Our sensors uncovered dozens of wireless networks that appeared to be operating without the awareness of site operators or infrastructure managers. These were not merely devices added temporarily or left undocumented, many of them represented entire communication frameworks operating autonomously in parallel to the known infrastructure. This unchecked expansion of wireless connectivity creates fractured trust zones, where devices communicate outside the purview of centralized monitoring or security policies. It is in these undefined spaces that attackers find opportunity, exploiting visibility gaps to pivot, persist, or exfiltrate with minimal resistance.

#802.15.4 Assets



In parallel, access point scans revealed deployments from over 50 distinct vendors, many of which are consumer or prosumer grade. In the chart below we report only the top 15 for sake of clarity, however these are not minor details. Each unknown device or rogue network represents a blind spot, and in ICS environments, blind spots can become pivot points.

Access Point Vendor Distribution



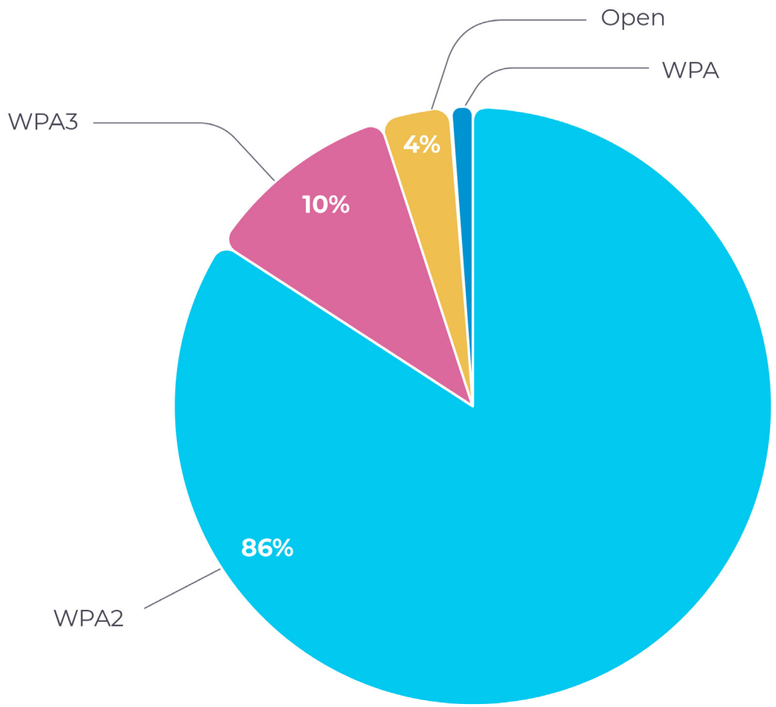
3.3 Weak Wireless Hygiene: Encryption Doesn't Equal Security

Even when wireless infrastructure is known and acknowledged within the organization, its actual security posture is often misunderstood or overestimated. Many assume that simply having WPA2 enabled or using passwords on access points equates to strong wireless security. However, wireless communication is inherently dynamic and decentralized — devices come and go, access points can be misconfigured, and protections meant to ensure confidentiality and integrity are frequently missing or improperly applied. A closer look at authentication methods and encryption schemes reveals the real level of risk beneath the surface.

Roughly 4% of observed wireless networks are operating with legacy or open configurations. This indicates a systemic weakness in a significant subset of the environment, where encryption standards are either outdated or entirely absent. These networks are highly exposed to common wireless threats such as sniffing, spoofing, and replay attacks, not due to sophisticated exploitation, but because their foundational security measures are no longer adequate.

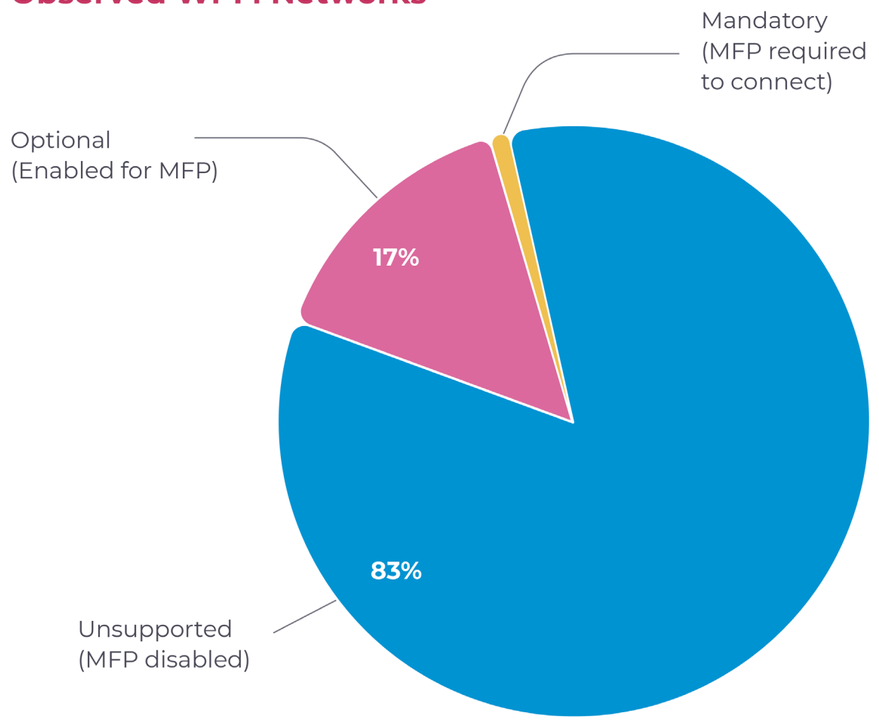
Although still limited, WPA3 adoption introduces significant advantages in mitigating these types of attacks. Features such as individualized data encryption, stronger handshake protocols and protection against brute-force attempts create a much stronger baseline of wireless resilience. As discussed in our previous report, WPA3 also mandates the use of 802.11w, which enforces Management Frame Protection (MFP) and prevents deauthentication attacks at the protocol level, significantly elevating the integrity of wireless session management.

Wi-Fi Encryption Protocols Distribution



But the issue runs deeper. Many WPA2-protected networks are missing basic protections like Management Frame Protection (MFP), a critical feature that defends against manipulation of control frames — the underlying communication signals that manage how devices connect and stay connected to access points.

802.11w MFP Configuration Status Across Observed Wi-Fi Networks



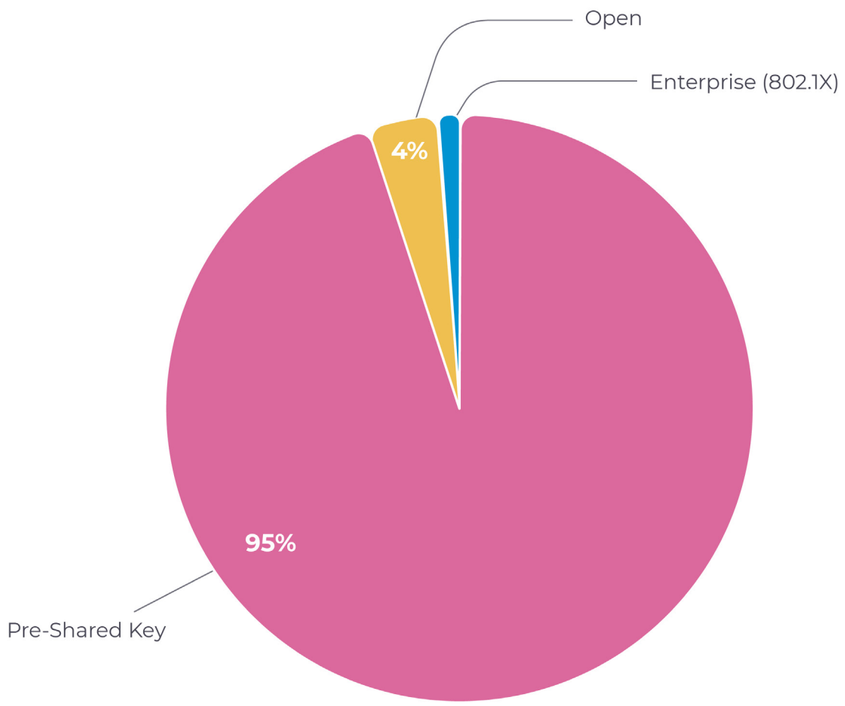
Compared to the second half of 2024, networks providing optional MFP support to clients increased by 17%, showing greater focus on security.

However, 83% of networks still lack MFP entirely. Without it, attackers can exploit well-known techniques like spoofing or deauthentication floods to disconnect devices, impersonate access points, or silently interfere with wireless traffic.

These tactics don't require breaking encryption — they exploit the blind trust in control-plane messaging that, without MFP, remains unprotected even in otherwise "secure" networks.

Even worse, 95% of Wi-Fi networks authenticate via shared passwords (PSK), while only a small fraction rey on secure enterprise-grade authentication methods such as 802.1X:

Wi-Fi Authentication Methods Distribution



This creates an environment where the entire wireless footprint is vulnerable to a cascade of risks that extend well beyond simple misconfiguration. Shared passwords mean that credentials are often reused across devices and personnel, eliminating any form of user attribution. In the event of a breach or suspicious activity, it becomes nearly impossible to trace actions to a specific individual or device. This lack of accountability weakens incident response, hampers forensic investigations, and allows lateral movement to go undetected. Furthermore, the overreliance on static credentials fosters a false sense of perimeter control, encouraging assumptions that a single layer of encryption is sufficient. These conditions enable threat actors to exploit wireless connectivity as a backdoor into otherwise segmented environments.

The RF spectrum is not a theoretical concern, but an active and expanding component of modern operational environments. From passive threats such as unauthorized data leakage and signal interference to active attack vectors like spoofing, jamming and backdoor access, wireless communication represents one of the most underestimated and least monitored dimensions of the threat landscape.

Organizations that neglect wireless telemetry are not simply missing logs or alerts; they are overlooking an entire operational reality. Critical infrastructure depends on situational awareness across all layers, and the wireless domain is no exception.

4. Telemetry and Threat Trends in 1H 2025

4.1 MITRE ATT&CK Techniques

There are many ways attackers can perform various stages of an attack to achieve their goals, and even one missed attack vector can lead to a breach. With so much pressure to not miss anything, it is more important than ever to be able to focus and address the most pressing issues first. Each organization should build their security program focusing on their organization's cybersecurity priorities, but businesses who use world-class telemetry and threat intelligence are better able to identify how to prioritize those issues.

In this section, we share the most common techniques, tactics and procedures (TTPs) observed globally in the first half of 2025 by region and industry, based on anonymized telemetry from our participating customers.

The following table identifies the top 10 MITRE ATT&CK techniques used by attackers in the first half of 2025.

Top 10 MITRE ATT&CK® Techniques

ID	Technique name	Tactics	%
T1498	Network Denial of Service	Impact	**17.6%**
T0814	Denial of Service	Inhibit Response Function	**17.4%**
T1557	Adversary-in-the-Middle	Credential Access; Collection	**16.0%**
T0846	Remote System Discovery	Discovery	**11.4%**
T0841	Network Service Scanning	Discovery	**11.4%**
T1110	Brute Force	Credential Access	**7.36%**
T0812	Default Credentials	Lateral Movement	**5.27%**
T0859	Valid Accounts	Persistence; Lateral Movement	**5.27%**
T1565	Data Manipulation	Impact	**4.11%**
T1071	Application Layer Protocol	Command And Control	**1.33%**

As we can see, various Denial of Service (DoS) attacks lead the chart in the first half of 2025. They aim to bring down important systems and cause damage to victim organizations. This can be particularly devastating for OT environments, where shutting down certain systems can be a long, costly and sometimes dangerous process. They are followed by the Adversary-in-the-Middle attacks, also known as Man-in-the-Middle (MITM) attacks. Generally, they involve the attackers inserting themselves between two communicating parties, in an attempt to compromise the confidentiality or integrity of the data. Remote System Discovery and Network Service Scanning techniques take fourth and fifth place, associated with attackers' attempts to understand the environment at the early stages of the attack.

Compared to the previous period, when the Data Manipulation and Application Layer Protocol techniques were the most common type of attacks, this time they close our chart, taking 9th and 10th places respectively. This reflects what we researchers and defenders have long observed: different threat actors and malware families dynamically emerge and recede, a constant reminder to have updated threat intelligence tailored to your industry and region. Continuous review and adaptation of available toolsets and how features are implemented is an investment in your ability to reduce risk, respond and recover when time and resources matter most.

4.2 Industry Insights

According to our telemetry, the top targeted industries (based on highest number of alerts per customer) were the following:

Transportation

Manufacturing

Business Services

Minerals & Mining

Energy, Utilities & Waste

Compared to the previous six-month period, the Transportation sector now takes first place, outnumbering Manufacturing. This is a warning for all the companies that belong to this industry. We all know how much our society relies on transportation to maintain our daily operations, so it is crucial to make sure that it is properly protected against modern cyber threats.

The next two sectors also swapped their positions, with the Minerals & Mining industry now taking 4th place while Business Services increased its position to 3rd. The last sector, Energy, Utilities & Waste maintained its 5th position in our chart of the most affected industries over this period.

The following sections review which MITRE ATT&CK techniques attackers used the most when targeting organizations in these industries.

Transportation

Adversary-in-the-Middle attacks topped the list in monitored transportation organizations, contributing to more than a fifth of all attacks detected by our sensors during the first half of 2025.

ID	Technique name	Tactics	%
T1557	Adversary-in-the-Middle	Credential Access; Collection	**21.4%**
T0846	Remote System Discovery	Discovery	**12.6%**
T0841	Network Service Scanning	Discovery	**12.6%**
T1498	Network Denial of Service	Impact	**12.5%**
T0814	Denial of Service	Inhibit Response Function	**12.4%**

Manufacturing

In the Manufacturing sector, the top five most common techniques mirrored the order observed across all industries globally.

ID	Technique name	Tactics	%
T1498	Network Denial of Service	Impact	**17.7%**
T0814	Denial of Service	Inhibit Response Function	**17.6%**
T1557	Adversary-in-the-Middle	Credential Access; Collection	**16.3%**
T0846	Remote System Discovery	Discovery	**11.2%**
T0841	Network Service Scanning	Discovery	**11.2%**

Business Services

In the Business Services sector, brute-force attacks (where attackers attempt to guess credentials to gain access) contributed to more than a third of attacks.

ID	Technique name	Tactics	%
T1110	Brute Force	Credential Access	**37.6%**
T1498	Network Denial of Service	Impact	**15.8%**
T0814	Denial of Service	Inhibit Response Function	**15.8%**
T0846	Remote System Discovery	Discovery	**8.59%**
T0841	Network Service Scanning	Discovery	**8.59%**

Minerals & Mining

The same top five techniques as Business Services were observed within the Minerals & Mining sector, with differing proportions.

ID	Technique name	Tactics	%
T1110	Brute Force	Credential Access	**18.6%**
T1498	Network Denial of Service	Impact	**18.1%**
T0814	Denial of Service	Inhibit Response Function	**18.0%**
T0846	Remote System Discovery	Discovery	**10.9%**
T0841	Network Service Scanning	Discovery	**10.9%**

Energy, Utilities & Waste

In the Energy, Utilities & Waste sector, various types of DoS attacks contributed to over three-quarters of observed attacks.

ID	Technique name	Tactics	%
T1498	Network Denial of Service	Impact	**38.4%**
T0814	Denial of Service	Inhibit Response Function	**38.4%**
T0846	Remote System Discovery	Discovery	**5.59%**
T0841	Network Service Scanning	Discovery	**5.59%**
T1565	Data Manipulation	Impact	**4.37%**

To summarize, the top techniques used by attackers vary by industry and change dynamically over time.

4.3 Regional Insights

According to our telemetry, during the first half of 2025 the top targeted countries (based on highest number of alerts per customer) were:

1	**Japan**	4	**Australia**
2	**Germany**	5	**Italy**
3	**Brazil**	6	**United States**

As in our previous report, we focused only on countries where we have statistically significant number of organizations sending us data.

Compared to the previous period, we can see a few notable changes. First and foremost, Japan now leads this list, while the U.S. fell from first to sixth place. While we generally review top 5 targeted countries, we have included a more detailed analysis of the U.S. due to significant threat actor activity related to the conflict in **Iran.**

Meanwhile, Germany moved from third to second place, and Brazil entered the list in third place. Australia remained in fourth position and Italy returned to the chart in fifth place after falling off for six months.

Let's take a look at each of these countries in greater detail.

Japan

In Japan, the Adversary-in-the-Middle technique was the most common attack executed by attackers, contributing more than a fifth of raised alerts. Various DoS attacks are next, with Default Credentials and Valid Accounts closing out the top five.

ID	Technique name	Tactics	%
T1557	Adversary-in-the-Middle	Credential Access; Collection	**21.7%**
T1498	Network Denial of Service	Impact	**18.1%**
T0814	Denial of Service	Inhibit Response Function	**17.8%**
T0812	Default Credentials	Lateral Movement	**12.6%**
T0859	Valid Accounts	Persistence; Lateral Movement	**12.6%**

Germany

Here, the Remote System Discovery and Network Service Scanning techniques, both discovery tactics, were most prevalent, together contributing to more than half of all detected attacks. The discovery phase is fundamental for attackers to execute a successful attack later, so it is crucial to proactively identify and mitigate this activity. Active polling can help.

Over the last few years, the OT security space has matured to the point where Active Polling technologies are now more robust and well tested. Vendors

ID	Technique name	Tactics	%
T0846	Remote System Discovery	Discovery	**28.4%**
T0841	Network Service Scanning	Discovery	**28.4%**
T1498	Network Denial of Service	Impact	**18.2%**
T0814	Denial of Service	Inhibit Response Function	**18.2%**
T0812	Default Credentials	Lateral Movement	**1.76%**

are delivering active features which are based on documented, supported capabilities of specific devices and the polling traffic is almost indiscernible from the hardware manufacturer's own implementations. Extensive field testing and monitoring have proven the reliability of active strategies to the point where organizations should no longer err on the side of caution with these technologies. Selecting products that support adaptive learning and active polling is a proven way to increase returns of ongoing, automated discovery and provide near real-time data for analysis. These features and practices uplift the effectiveness of security operations.

Brazil

In Brazil, more than half of the detected attacks included various DoS techniques.

It is extremely important for businesses relying on their systems to be reliably up and running to invest time and effort into early detection and prevention of these techniques. Here, preference should be given to solutions that support various types of procedures implementing these techniques.

ID	Technique name	Tactics	%
T1498	Network Denial of Service	Impact	**26.1%**
T0814	Denial of Service	Inhibit Response Function	**26.1%**
T1557	Adversary-in-the-Middle	Credential Access; Collection	**22.2%**
T1110	Brute Force	Credential Access	**8.59%**
T0812	Default Credentials	Lateral Movement	**3.20%**

Australia

In contrast, Australia suffered most from weak credential issues.

ID	Technique name	Tactics	%
T0812	Default Credentials	Lateral Movement	**22.8%**
T0859	Valid Accounts	Persistence; Lateral Movement	**22.8%**
T1557	Adversary-in-the-Middle	Credential Access; Collection	**10.6%**
T1498	Network Denial of Service	Impact	**8.88%**
T0814	Denial of Service	Inhibit Response Function	**8.88%**

Companies that proactively embrace essential cybersecurity hygiene can significantly safeguard their operations and prevent widespread security breaches. This involves the critical steps of changing default credentials, implementing strong credential management and providing thorough user education.

Italy

In Italy, Data Manipulation contributed to more than a third of all detected incidents.

ID	Technique name	Tactics	%
T1565	Data Manipulation	Impact	**36.7%**
T0812	Default Credentials	Lateral Movement	**12.4%**
T0859	Valid Accounts	Persistence; Lateral Movement	**12.4%**
T1110	Brute Force	Credential Access	**9.79%**
T1557	Adversary-in-the-Middle	Credential Access; Collection	**9.21%**

Each region faces different challenges, with their environments being more vulnerable to certain attacks. Once some issues are fixed, the next ones should be immediately prioritized. We encourage readers to follow our recommendations at the end of the report for actionable advice.

United States

Despite the U.S. falling to 6th place during this period, recent Iran-related events merit a review in greater detail. Nozomi Networks Labs observed a 133% increase in activity of Iranian-linked actors targeting the United States. This increase in cyberattacks between May and June has been linked to well-known Iranian threat actor groups. From what we have observed so far, U.S. companies appear to be the primary target, as warned by CISA and the U.S. Department of Homeland Security. More information can be found in our **related blog post.**

Here are the top 5 most common MITRE ATT&CK techniques that all the attackers used to target US-based companies in the first half of 2025.

ID	Technique name	Tactics	%
T1498	Network Denial of Service	Impact	**24.2%**
T0814	Denial of Service	Inhibit Response Function	**24.0%**
T1110	Brute Force	Credential Access	**10.8%**
T0846	Remote System Discovery	Discovery	**9.61%**
T0841	Network Service Scanning	Discovery	**9.61%**

Various Denial of Service (DoS) attacks dominated the threat landscape during this period, accounting for over 48% of all the alerts raised. Brute Force technique followed, associated with attackers attempting to obtain access to the victim systems trying multiple variants of potentially working credentials.

We continue to closely monitor the situation and share our findings with the public, as well as update our Threat Intelligence feed. Nozomi Networks customers with access to our Threat Intelligence subscription are covered for these attacks.

4.4 Endpoint Telemetry: The Hidden Layer of Operational Risk

In industrial and critical infrastructure environments, endpoints represent a vital yet often under-monitored layer of the security architecture. These devices serve as operational touchpoints where digital processes intersect with physical ones — making them a primary conduit for lateral movement, payload execution and operator-targeted attacks. From engineering workstations and maintenance laptops to mobile diagnostic tools, endpoints are exposed to diverse threat surfaces that transcend traditional IT boundaries.

What makes endpoints particularly challenging in this context is their dual role: they are both essential to operations and inherently vulnerable due to their mobility, user interaction and connectivity. While perimeter defenses and network monitoring provide valuable visibility, many attack vectors — especially those involving human access, physical ports or local scripting — exploit blind spots at the endpoint level. Among these, USB-based threats stand out as a persistent and underestimated risk.

According to telemetry collected across our deployed sensors, the following suspicious activity was detected the most in our customers' endpoints:

Suspicious activity	%
USB file transfer	**81.9%**
Malicious USB device	**10.5%**
New USB device plugged	**7.58%**
Malicious Human Interface Device	**0.0325%**

These figures are not just statistically significant, they are operationally urgent. USB devices continue to be used as entry points for malware, often bypassing traditional network detection. The chart above highlights key telemetry signals: 10.5% of alerts involved clearly malicious USB devices, while an additional 7.58% were triggered by newly connected devices — often the first indicator of risky or unauthorized behavior. Together, these categories represent a spectrum of abuse that spans from overt to stealthy, making USB monitoring essential at both the hardware and behavioral level.

The threat is especially acute in OT environments where endpoints are physically accessible, security agents may be absent, and asset hardening is inconsistent. These types of USB-based threats may also play a role in air-gapped attack scenarios, facilitate rogue insider actions, or serve as a vector for accidental exposure introduced via compromised supply chain components. In some well-documented cases, USB-delivered malware has been used to cross isolated environments, exploit trust assumptions in removable media, and enable adversaries to establish a persistent foothold — all without requiring network connectivity or external communication.

But USB-based threats are only one piece of the endpoint puzzle. Another often-overlooked dimension is how legitimate tools are misused post compromise to maintain stealth and persistence.

Malware Category	%
Dual Use	**99.97%**
Ransomware	**0.03%**

This is where the concept of dual-use tooling becomes highly relevant. In cybersecurity, dual-use refers to legitimate system utilities and administrative tools that serve essential operational purposes but can be repurposed by attackers for malicious ends. These include scripting engines like PowerShell, diagnostic tools like the Sysinternals Suite and file system utilities such as fsutil.

Because these tools are native, signed and often allowlisted, adversaries exploit them post-compromise to blend in with routine system activity, avoid detection, and execute advanced tactics without introducing traditional malware.

In our endpoint telemetry, one detection rule related to PowerShell-based downloads was triggered nearly 50,000 times within the reporting period. This alone highlights how often adversaries lean on native scripting environments to stage payloads, exfiltrate data or initiate further lateral movement — all without deploying conventional malware. Usage of the SysInternals Suite came in second place, followed by deletion of Windows security logs.

Looking at all the threats detected by our behavioral detection engine, the numbers for RANSOMWARE bring immediate attention. Despite comprising only 0.03% of detected attacks, if any of these attacks remaining undetected have the potential to be extremely damaging for the victim.

Unlike traditional malware, which relies on recognizable signatures, dual-use techniques exploit trusted binaries, making them far harder to detect without behavioral analytics and contextual telemetry. This is especially dangerous in environments where endpoint logging is minimal or absent, leaving defenders blind to adversary actions that appear legitimate on the surface.

The implication is clear: monitoring for dual-use behavior is not optional — it's essential. Visibility into how native tools are executed, under what conditions and by which users provides the missing link for detecting stealthy intrusions and preventing post-compromise activity from escalating into full-scale incidents.

5. Vulnerability Landscape and Exploitability Trends

5.1 Top CVEs Affecting Customer Environments

This section shares how vulnerabilities published in the first half of 2025 are distributed in our customers' environments around the globe.

CVE ID	CVSS score	CWE
CVE-2025-5419	8.8	CWE-125 <Out-of-bounds Read>
CVE-2025-5066	6.5	CWE-451 <User Interface (UI) Misrepresentation of Critical Information>
CVE-2025-5958	8.8	CWE-416 <Use After Free>
CVE-2025-5959	8.8	CWE-843 <Access of Resource Using Incompatible Type ('Type Confusion')>
CVE-2025-5063	8.8	CWE-416 <Use After Free>
CVE-2025-5283	5.4	CWE-416 <Use After Free>
CVE-2025-5068	8.8	CWE-416 <Use After Free>
CVE-2025-5064	5.4	CWE-200 <Exposure of Sensitive Information to an Unauthorized Actor>
CVE-2025-5280	8.8	CWE-787 <Out-of-bounds Write>
CVE-2025-5067	5.4	CWE-290 <Authentication Bypass by Spoofing>

Six of the top 10 CVEs have a CVSS risk score of 8.8 (high), representing a significant threat. Other vulnerabilities have a lower risk score, but many either don't require authentication or let attackers bypass it, making them easier to exploit. We encourage companies to immediately revise vulnerabilities they discovered in their environment and remediate them as soon as possible as there is a very high chance attackers may target them. Please explore the recommendations at the bottom of the report for more information.

Next, let's look at the most common categories of vulnerabilities published in 2025.

5.2 Top CWEs in Customer Environments

CWE (Common Weakness Enumeration) is a standardized system for identifying and categorizing software weaknesses and vulnerabilities. The following table lists the most common categories of vulnerabilities identified by the Nozomi Networks platform in customer environments that were published in the first half of 2025, in descending frequency.

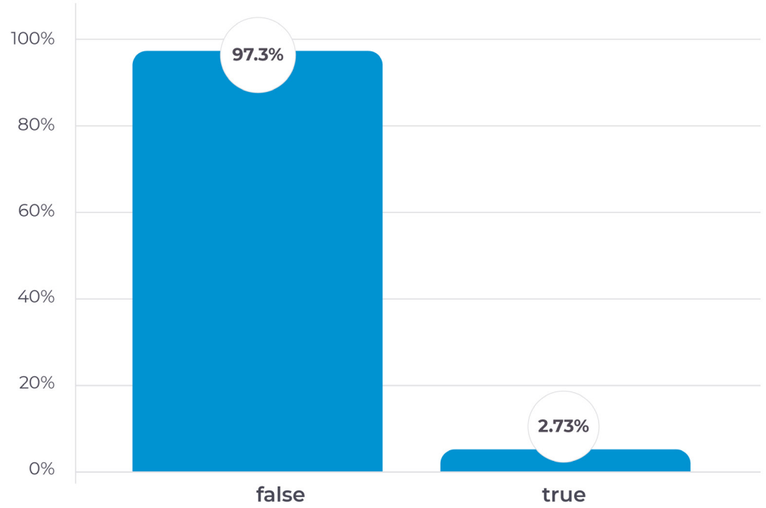
CWE	Percentage
CWE-416 <Use After Free>	17.4%
CWE-125 <Out-of-bounds Read>	13.5%
CWE-122 <Heap-based Buffer Overflow>	10.3%
CWE-451 <User Interface (UI) Misrepresentation of Critical Information>	5.69%
CWE-200 <Exposure of Sensitive Information to an Unauthorized Actor>	4.86%
CWE-787 <Out-of-bounds Write>	4.05%
CWE-843 <Access of Resource Using Incompatible Type ('Type Confusion')>	3.42%
CWE-79 <Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')>	3.08%
CWE-1021 <Improper Restriction of Rendered UI Layers or Frames>	3.04%
CWE-290 <Authentication Bypass by Spoofing>	2.87%

Topping the chart are the notorious Use-After-Free vulnerabilities, associated with situations when some memory was freed but later, due to a logic bug, it was accessed again. Attackers may abuse this vulnerability to achieve arbitrary code execution, perform DoS attacks or leak sensitive information. Next are Out-of-bounds Read attacks. They happen when, due to a bug, a program may attempt to read more information than the size of the data buffer, leading to various unexpected outcomes. Heap-based Buffer Overflow comes in third, a reminder that buffer overflows are far from being extinct in 2025.

5.3 Top KEV and EPSS Scores in Customer Environments

Known Exploited Vulnerabilities (KEVs) are a status assigned by CISA to vulnerabilities that are confirmed to be targeted by malicious actors, and they should be patched by U.S. federal agencies by a given deadline. The table below identifies the most recent vulnerabilities in our customers' environments marked as KEVs.

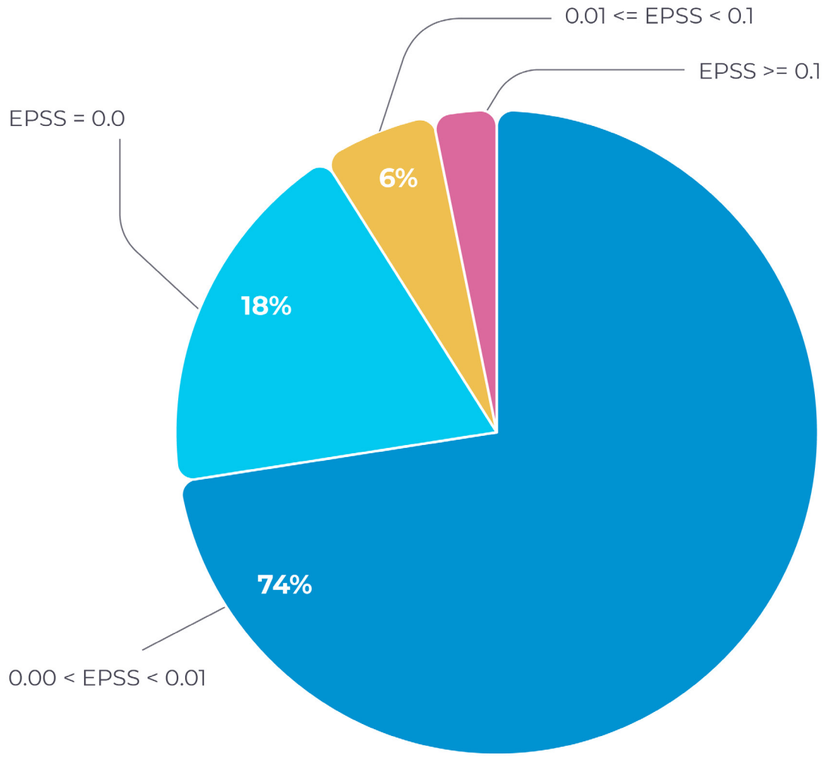
Percentage of 2025 vulnerabilities found in real environments marked as KEV



The low number shouldn't be underestimated – each of them may give attackers access to sensitive data or let them cause other types of damage. Secondly, KEVs are not synonymous with all vulnerabilities that were confirmed to be actively exploited, and they don't explicitly specify the chances that some particular vulnerability is going to be exploited. To better understand that aspect, we need to explore another metric, the Exploit Prediction Scoring System (EPSS).

Almost three-quarters of identified vulnerabilities have EPSS scores representing the probability of exploitability between 0% and 1%. Organizations may want to prioritize ones that have an EPSS score higher than 1% when they perform vulnerability management.

Distribution of 2025 Vulnerabilities by EPSS Score



6. Botnet Activity in OT/IoT Environments

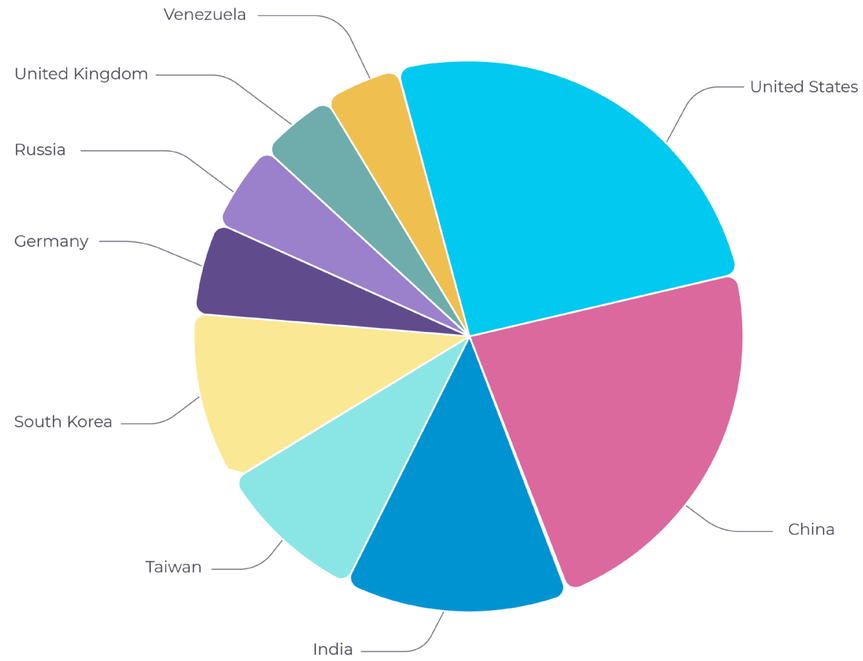
In this section, we analyze botnet activity statistics obtained from Nozomi Networks Labs' chain of globally distributed IoT honeypots. This data comes not from our telemetry but from dedicated sensors simulating vulnerable devices, letting bots execute various stages of attacks and providing us with invaluable insights for better protecting our customers.

6.1 Attack Source Locations

First, let's take a look at where the attacks originated, based on the location of the public IP address associated with the attack. Each unique IP address is counted only once during this period, enabling us to estimate how many compromised devices are in each country compared to others:

Distribution of Attacks Based on IP Address Origin

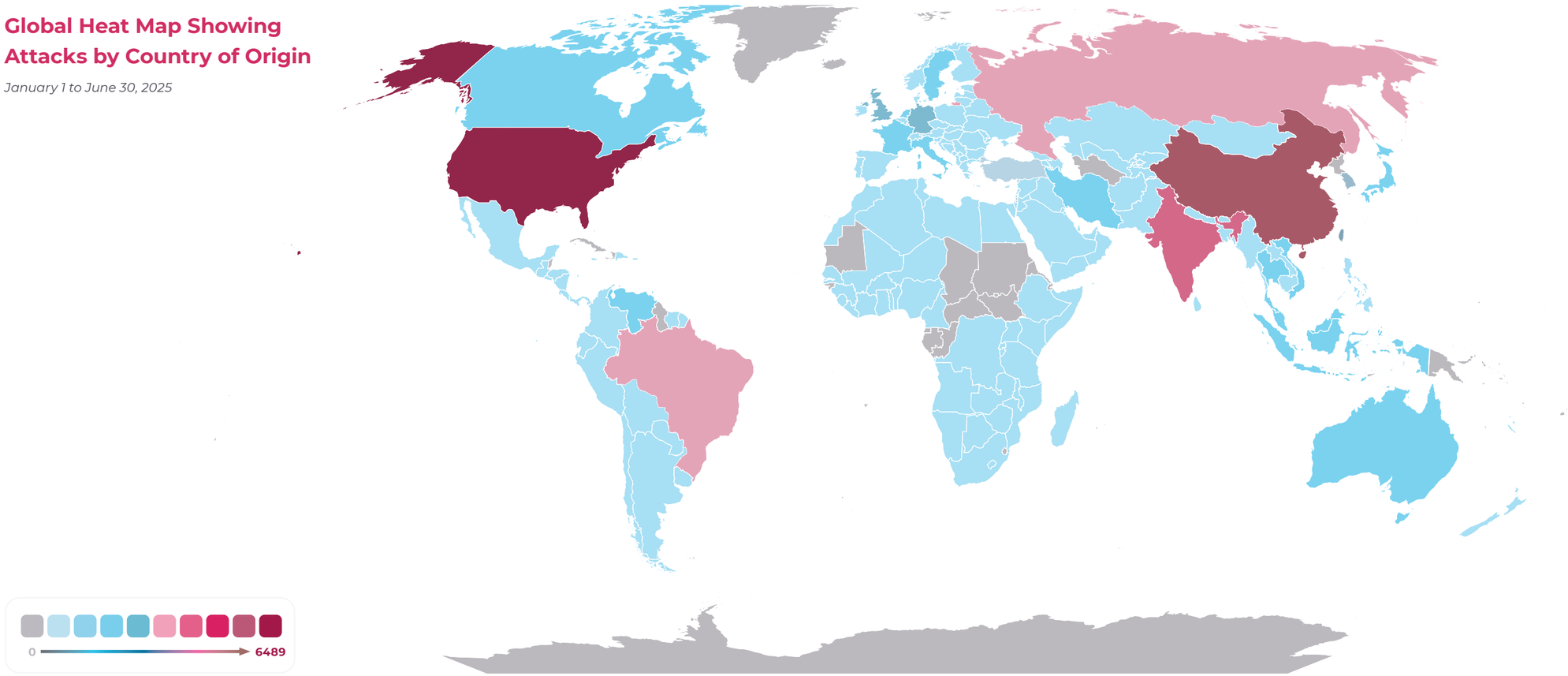
January 1 to June 30, 2025



Here is how this data looks in a heatmap:

Global Heat Map Showing Attacks by Country of Origin

January 1 to June 30, 2025



Compared to the previous period, the U.S. overtook China as having the most compromised devices originating attacks. This is first time China hasn't been in first place since at least 2022, when we started monitoring this activity. We recommend all U.S. organizations take measures to ensure their IoT devices are not part of any malicious botnets. Next, we review how active these botnets were over the first half of 2025.

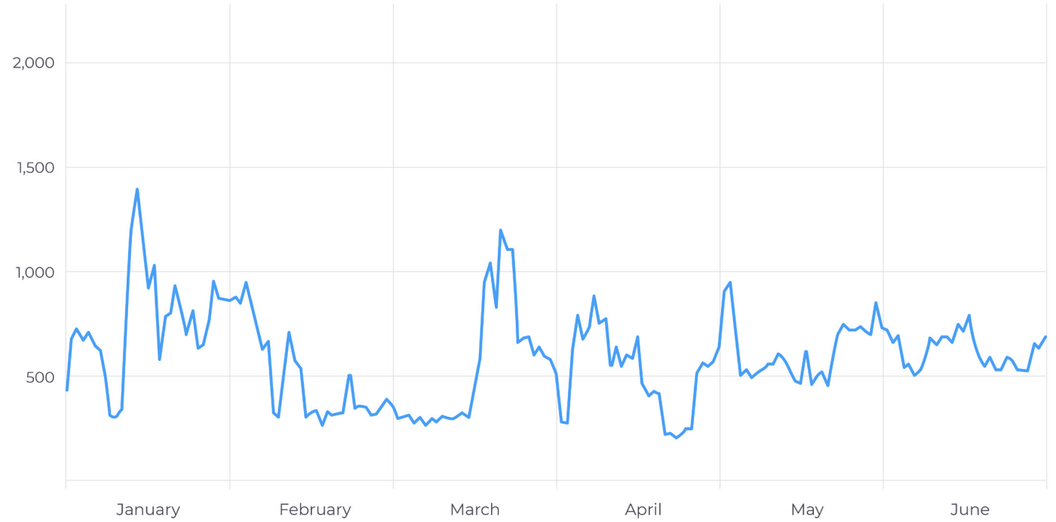
6.2 Number of Unique Daily Attacker IPs

Botnets are dynamic structures, with new bots being added when new devices are compromised and removed when they are remediated. We counted the attacks coming from unique locations (based on public IP addresses) over time to understand when they were most active.

Botnet activity peaked on January 17, when we recorded attacks originating from 1,429 different IP addresses in one day. This is slightly below the highest peak in the previous period, when we recorded 1,595 unique botnet IP addresses in one day in September 2024. This spike was associated with a known Mirai-based botnet that was particularly active on that day. Tracking such spikes allows us to promptly update our detections when we notice a new undetected strain of malware, which in turn delivers increased protection for our customers.

Daily Volume and Activity from Unique Attacker IP Addresses

January 1 to June 30, 2025

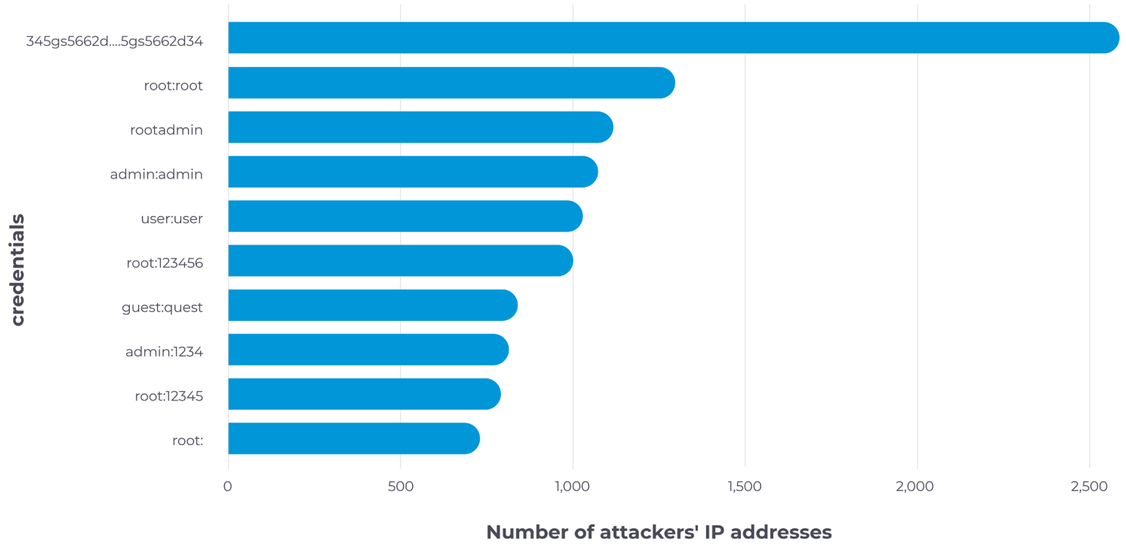


6.3 Top Credentials Used

One of the most common ways IoT botnets propagate is by brute-forcing known credentials to establish initial access. Let's look at the most commonly used pairs:

Top Credentials Used by Attackers for Initial Access to Honeypots

January 1 to June 30, 2025



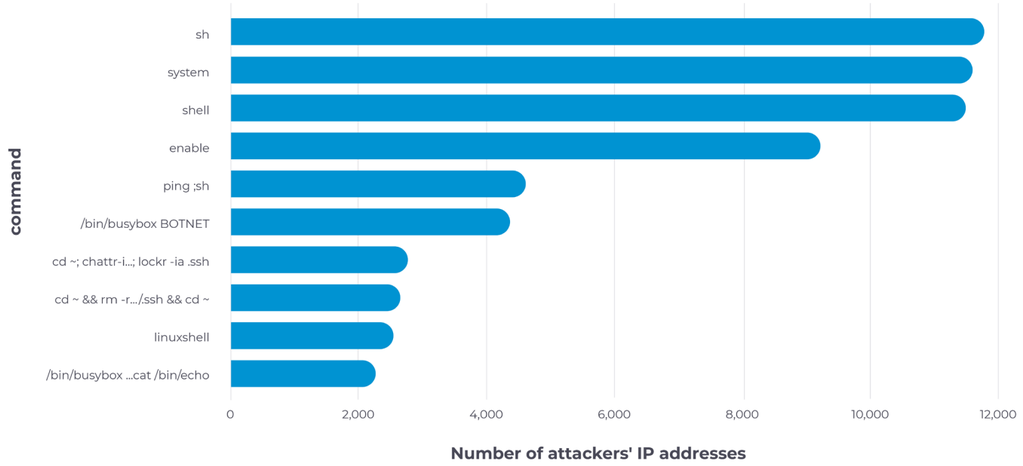
Few surprises here: accounts associated with the privileged users such as root or admin continue to be the most prevalent. Device manufacturers intentionally set defaults to users with high privileges to simplify device management. Unless they are changed immediately as part of routine cyber hygiene, these default passwords hand attackers easy access.

Once initial access is established, attackers generally start executing additional payloads and custom commands. Let's review the most popular ones.

6.4 Top Executed Commands

Top 10 Post-Access Commands by Number of Bots Executing Them

January 1 to June 30, 2025



Many of these commands (sh, system, shell, enable, busybox, linuxshell) are just needed to establish the right shell. A few others are more interesting. The "cd ~; chattr -ia .ssh; lockr -ia .ssh" command indicates attackers are using the standard chattr tool (renamed to lockr) to change permissions for the standard .ssh folder, which contains allowed SSH keys. In the long command, attackers are trying to astore their public key in the .ssh folder so they can return at any time.

Here is a full list:

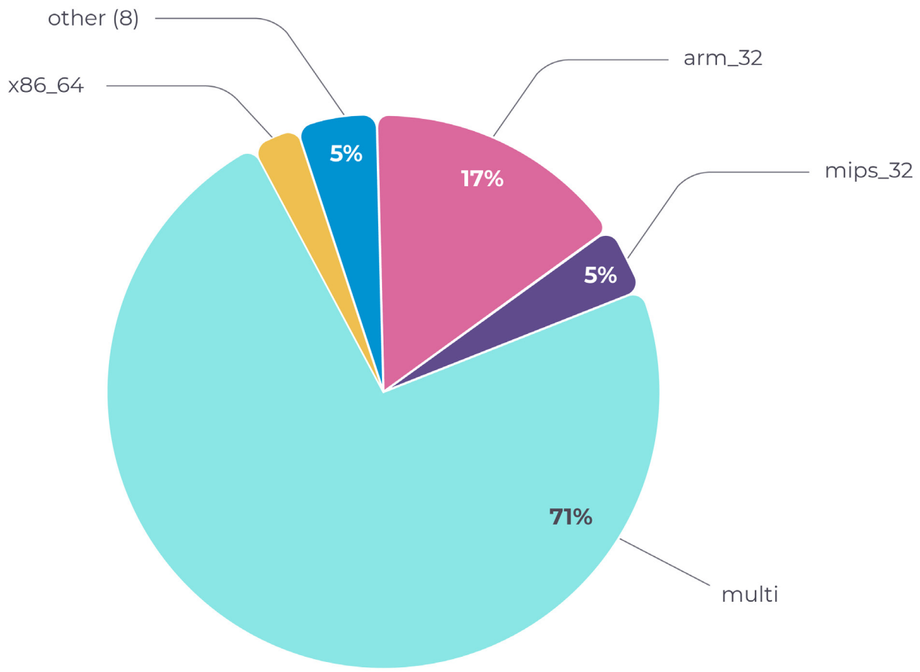
- **sh**
- **system**
- **shell**
- **enable**
- **"ping ;sh"**
- **"/bin/busybox BOTNET"**
- **"cd ~; chattr -ia .ssh; lockr -ia .ssh"**
- **"cd ~ && rm -rf .ssh && mkdir .ssh && echo ""ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli 2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUanUV9tJ2/9p7+vD0EpZ3Tz /+0kX34uAx1RV/75GVOmNx+9EuWOnvNoaJe0QXxziIg9eLBHpgL Muakb5+BgTFB+rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEm PecjdySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCGP K5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujvcD9iUKQTTWYY jIIu5PmUux5bsZ0R4WFwdIe6+i6rBLAsPKgAySVKPRK+oRw== mdrfckr """>>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~"**
- **linuxshell**
- **"/bin/busybox cat /proc/self/exe || cat /bin/echo"**

6.5 Top Payload File Types

Very often, once a system is compromised, attackers deliver either shell scripts or compiled executables. Looking at payload architecture, we see the following picture:

Top Payload Types by Targeted Architecture

January 1 to June 30, 2025



Apart from the “multi” category, which various shell scripts belong to, attackers attempted to deploy 32-bit ARM payloads most frequently, followed by 32-bit MIPS. Surprisingly 64-bit x86 (vs. 32-bit) took third place, signifying wide adoption of this type of CPUs in the IoT domain. Finally, 32-bit POWER (an evolution of PowerPC) and other x86 architectures rounded out the top five most popular payloads.

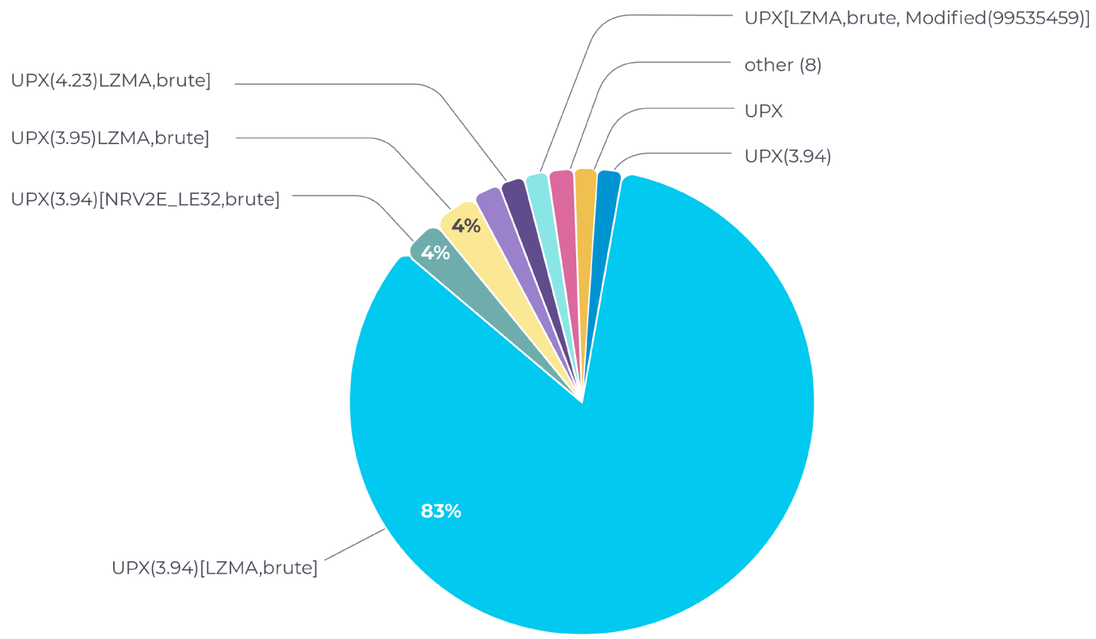
As a reminder, don’t assume your devices are safer just because they use less popular and therefore less-targeted architectures. Attackers can easily target less common architectures, so hoping that attackers don’t know how to penetrate them is ineffective. Prioritize vulnerabilities across all architectures in your environment if you want to reduce risk.

6.6 Top Payload Packers

Some attackers attempt to protect their payloads from being detected by applying various types of packers. Here are the most widely used ones.

Top Packers Used to Protect Malicious Payloads

January 1 to June 30, 2025



Despite being a few years old, UPX 3.94 is still used by most attackers to protect their creations. Introduced last year, UPX 4.2.3 comes in second, with other packers used much less often. We will continue to watch this area, making sure the Nozomi Networks platform can unpack observed executables, and use signatures like YARA rules to efficiently detect malicious ones.

7. Strategic Recommendations

As this report emphasizes, the modern threat landscape requires a shift from static to dynamic security measures, reinforced network segmentation and robust continuous asset monitoring.

Adhering to established best-practice frameworks will help you detect threats that would otherwise remain under the radar. By embracing these strategies, critical infrastructure and other ICS operators can successfully build resilience against the evolving spectrum of OT- and IoT-specific cyber threats.

Implement a Risk Reduction Strategy

This approach involves identifying, assessing, and prioritizing cybersecurity risks based on multiple factors such as their potential to cause significant damage as well as the probability of it happening. By aligning mitigation efforts with the organization's risk tolerance and critical assets, this strategy not only reduces the likelihood and impact of cyber threats but also supports compliance with regulatory requirements and enhances operational resilience.

With malware causing multimillion-dollar losses to victim companies, it's important to keep your threat intelligence databases updated and ensure that your security providers prioritize OT and IoT threats.

Prioritize Anomaly Detection and Response

With nation-state threat actors relying on living-off-the-land tactics and malware inflicting multimillion-dollar losses on victim companies, keeping threat intelligence databases up to date is critical to safeguard against known threats. However, signature-based detection alone may not suffice for emerging or unknown threats. Many reconnaissance activities are more effectively uncovered through anomaly detection rather than purely signature-based approaches.

It's therefore essential to adopt a multi-layered defense strategy and deploy solutions capable of identifying abnormal behavior that deviates from your established baselines.

Adopt Regional and Industry-specific Threat Intelligence

Focus on targeted threat intelligence to identify the unique risks your industry and region face.

Tailor the security measures based on insights into regional attack trends and sector-specific vulnerabilities, prioritizing resources for maximum impact and risk reduction.

Strengthen Wireless Network Security With Regular Audits

Conduct comprehensive wireless security audits to identify potential vulnerabilities in industrial wireless environments. Prioritize mitigating common threats, such as deauthentication attacks, by deploying robust encryption protocols and isolating sensitive networks. Leverage security solutions with wireless monitoring capabilities and take immediate mitigation actions upon threat detection to ensure operational continuity.

Enhance Vulnerability Management With Key Metrics

Implement a proactive vulnerability management program that not only prioritizes vulnerabilities with high-risk scores but also takes into account asset criticality, compensating controls, device type, safety implications, exposure and other contextual factors. This approach ensures resources are allocated effectively and addresses the most pressing threats first, maximizing your organization's overall security posture.

Fortify Defenses Against Botnet Attacks

Recognize the growing threat of botnets targeting OT/IoT environments and adopt a multi-layered defense strategy. Use traffic analysis and anomaly detection tools to identify botnet activity early. Strengthen endpoint security and apply network segmentation to limit the reach of an attack from botnets, and safeguard and maintain operational continuity of critical infrastructure.

Work With Your Partners

Know that cyber defense is a team sport that requires deep bench strength. Get the knowledge and capabilities you need by bringing together internal operational and cyber practitioners, leaning on your vendors, following OT/ICS cybersecurity experts and participating in your industry's information sharing and analysis center (ISAC).

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com