NOZOMI NETWORKS LABS

2024 2H REVIEW

OT/IoT Cybersecurity Trends and Insights

February 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 Overview

Cyberattacks on the world's critical infrastructure are on the rise. Global tensions continue to escalate, ransomware operators act with impunity, geopolitical conflict rises, cyber-espionage persists, and cyber has become an integral part of military strategies. The systems we design and defend must not only withstand a barrage of threats in today's multipolar world but also balance the need to operate safely at scale, where human lives are at stake.

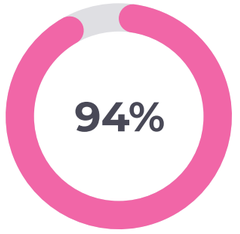
Multi-year adversarial operations such as Volt Typhoon and Salt Typhoon have recently been exposed, highlighting how nation-state actors have infiltrated critical infrastructure and communications systems, often remaining undetected for years.

The Nozomi Networks Labs team delivers this semi-annual report to provide insights into how the world's largest industrial organizations and critical infrastructure operators can protect themselves from these advanced threats. Leveraging a network of more than 50,000 global honeypots, wireless monitoring sensors, inbound telemetry, partnerships, threat intelligence and other resources, our team uncovers trends, novel attack methods and unique insights that are critical for safeguarding operational technology (OT) and cyber-physical systems.

While cybersecurity reports often focus on threats targeting wired networks—such as Ethernet, industrial Ethernet and fiber—our capabilities extend beyond wired networks to encompass a multitude of wireless transport protocols.

This expanded visibility enables our research team to access insights that are otherwise unavailable. Threats do not solely reside in Wi-Fi access points; wireless protocols like ZigBee, Bluetooth, LoRaWAN and others are heavily relied upon in industrial environments including power grids, transportation systems, security devices and medical equipment. Alarmingly, our findings reveal that 94% of Wi-Fi networks lack sufficient protections against deauthentication attacks, which are frequently leveraged as part of larger incidents. These vulnerabilities expose organizations to risks such as credential theft, traffic interception, man-in-the-middle attacks and spoofing, any of which could compromise the integrity of critical control systems.

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.



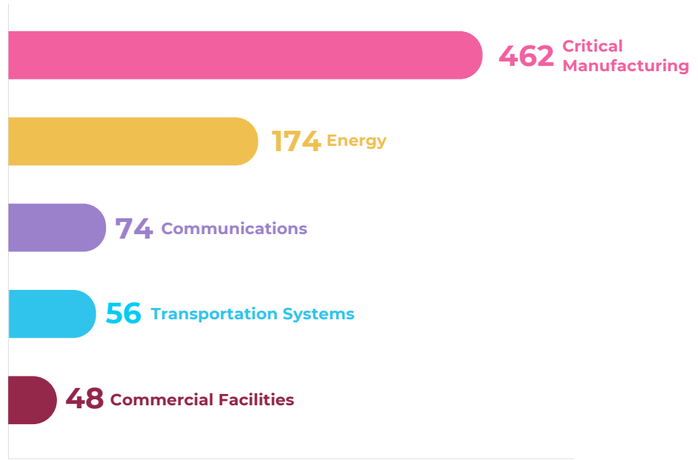
of Wi-Fi networks lack protection against deauthentication attacks

For example, manufacturing was the most targeted sector during the reporting period, and the U.S. was the most attacked country, up from #5 during the first half of 2024. Together these findings signal that U.S. manufacturers should increase their vigilance, as they are regularly targeted by ransomware and espionage campaigns.

In addition to reviewing the key threats from second half of 2024 such as malware, botnets and vulnerabilities, the report also delivers clear recommendations for how to navigate these emerging risks in the coming year.

By understanding these evolving threats and leveraging actionable insights, we can defend our critical systems to ensure resilience, safety and operational continuity in an increasingly uncertain world.

Most Targeted Sectors



Most Attacked Countries

	H1 2024	H2 2024
1	Italy	United States
2	Spain	Sweden
3	Colombia	Germany
4	Sweden	Australia
5	United States	Colombia

2. Introduction

In this report we analyze unique telemetry from hundreds of real OT and IoT environments to provide a comprehensive overview of the dynamic threat landscape in the second half of 2024. The report breaks out our findings by region and industry to help you fine-tune your defense strategies.

Because wireless network security has emerged as a critical factor in maintaining operational continuity, our latest research includes a special section that examines the hidden risks of industrial wireless environments, including threats such as deauthentication attacks, which can compromise critical systems and processes.

The results of a special security hygiene audit reveal common vulnerabilities and underscore why monitoring wireless networks is vital for protecting infrastructure.

We also explore broader trends in ICS asset vulnerability advisories, presenting key statistics on the top affected sectors and Common Weakness Enumerations (CWEs). We assess the current impact of botnet activity on IoT systems and provide guidance for protecting against this persistent threat. Finally, we dig into recent OT malware attack patterns — including new families such as *BUSTLEBERM* (also known as FrostyGoop) and *OrpaCrab* (also known as IOCONTROL) to give you the insights you need to keep your OT and IoT environments safe.

3. Threat Intelligence: Understanding Regional and Industry Risk Exposure

This section analyzes Nozomi Networks' anonymized telemetry from our participating customers to reveal top cybersecurity trends affecting key industries and regions across the world. All data was collected between July 1 – December 31, 2024.

Platform alerts have been translated to their corresponding MITRE ATT&CK tactics, techniques and procedures (TTPs), from both ICS and enterprise matrices.

The **Data Manipulation** technique leads the chart, occurring more than three times as often as the next most-detected threats. Various attacks performed over **Application** and **Non-Application protocols** placed 2nd and 3rd, respectively, followed by the **Network Denial of Service** technique, which represents various ways to disrupt network activity. Discovery phase techniques like **Network Service Scanning** and **Remote System Discovery** rank next, followed by **Adversary-In-The-Middle** (commonly known as MITM). **Brute Force** attacks, commonly used by attackers to try different combinations of credentials to establish initial access comprised 3.2% of alerts. Closely related **Default Credentials** and **Valid Accounts** techniques, which use legitimate credentials (often weak/default or stolen) to achieve initial access, made the top 10 list but accounted for less than 1% of alerts each.

Top 10 Most Common MITRE ATT&CK™ Techniques Associated with Raised Alerts

ID	Technique name	Tactic name	%
T1565	Data Manipulation	Impact	**39.54%**
T1071	Application Layer Protocol	Command and Control	**12.29%**
T1095	Non-Application Layer Protocol	Command and Control	**12.29%**
T1498	Network Denial of Service	Impact	**8.86%**
T0841	Network Service Scanning	Discovery	**7.89%**
T0846	Remote System Discovery	Discovery	**7.89%**
T1557	Adversary-in-the-Middle	Credential access; Collection	**5.48%**
T1110	Brute Force	Credential access	**3.20%**
T0812	Default Credentials	Lateral Movement	**0.89%**
T0859	Valid Accounts	Persistence; Lateral Movement	**0.89%**

These findings reinforce the need for industrial organizations to embrace a holistic approach to cybersecurity and prioritize their efforts according to the current global trends:

- Verify that your cybersecurity solution detects Data Manipulation-related attacks and provides you with enough context to act on them.
- Make sure your network is resilient to DoS attacks and can be easily restored in case of emergency.
- Don't ignore Discovery tactic-related techniques like Network Service Scanning. While seemingly benign, they can have big consequences during the later stages of an attack, providing malicious actors with all the information they need to succeed.
- Enforce strong credential management by immediately changing default credentials, forbidding weak passwords through company-wide policies and education, and ensure you can efficiently detect various types of Adversary-In-The-Middle attacks.

3.1 Industry Insights

Different industries face different challenges, and it's important to track them to provide fine-tuned solutions rather than following a one-size-fits-all approach. In this section, we look at the top techniques used by attackers in the most targeted industries.[1]

Here are the top general industries associated with the highest number of alerts per customer in the second half of 2024:

- Manufacturing
- Transportation
- Minerals & Mining
- Business Services
- Energy, Utilities & Waste

The following pages break down the top 5 MITRE ATT&CK techniques by sector according to available customer data during the reporting period.

Manufacturing

ID	Technique name	Tactic name	%
T1565	Data Manipulation	Impact	**59.57%**
T1498	Network Denial of Service	Impact	**9.62%**
T0841	Network Service Scanning	Discovery	**9.19%**
T0846	Remote System Discovery	Discovery	**9.19%**
T1557	Adversary-in-the-Middle	Credential access; Collection	**4.17%**

For the Manufacturing sector, more than half of all the reported attacks were associated with the Data Manipulation technique. It is followed by Network Denial of Service technique and closely related Network Service Scanning and Remote System Discovery techniques.

[1] As always, to avoid bias towards the number of Nozomi Networks customers has in different countries, these numbers are averaged on a per-customer basis. In addition, only the industries where Nozomi Networks has at least five customers are included.

Transportation

ID	Technique name	Tactic name	%
T1565	Data manipulation	Impact	26.72%
T1110	Brute Force	Credential access	17.11%
T1557	Adversary-in-the-Middle	Credential access; Collection	14.28%
T1498	Network Denial of Service	Impact	11.48%
T0875	Change Program State	Execution; Impair process control	8.86%

In the Transportation sector, the proportion of Data Manipulation-related attacks is more than twice as low as in the Manufacturing sector. In addition, Brute Force attacks were much more prevalent, comprising around 17% of all the reported attacks.

Minerals & Mining

ID	Technique name	Tactic name	%
T0841	Network Service Scanning	Discovery	37.97%
T0846	Remote System Discovery	Discovery	37.97%
T1498	Network Denial of Service	Impact	10.12%
T1565	Data manipulation	Impact	6.75%
T1200	Hardware Additions	Initial access	2.25%

Energy, Utilities & Waste

ID	Technique name	Tactic name	%
T1557	Adversary-in-the-Middle	Credential access; Collection	50.38%
T1110	Brute Force	Credential access	27.98%
T1498	Network Denial of Service	Impact	15.23%
T0841	Network Service Scanning	Discovery	1.58%
T0846	Remote System Discovery	Discovery	1.58%

Business Services

ID	Technique name	Tactic name	%
T1565	Data Manipulation	Impact	43.25%
T0841	Network Service Scanning	Discovery	22.96%
T0846	Remote System Discovery	Discovery	22.96%
T1498	Network Denial of Service	Impact	4.63%
T1557	Adversary-in-the-Middle	Credential access; Collection	3.98%

To summarize, different sectors pose different challenges. That's why it's so important to reinforce a comprehensive cybersecurity program with protection against the known threats facing your industry.

3.2 Regional Insights

Here, we look at the countries reporting the highest number of alerts per customer operating there. To avoid bias, only countries where Nozomi Networks has at least 5 customers are considered. Here is the top five ranking for the second half of 2024, compared to the previous six months:

	H1 2024	H2 2024
1	Italy	United States
2	Spain	Sweden
3	Colombia	Germany
4	Sweden	Australia
5	United States	Colombia

Compared to the previous 6-month period, the U.S. moved from 5th position to 1st, reflecting the relative increase in alerts in our U.S. customer environments compared to the first half of 2024. Sweden moved from 4th position to 2nd, while Colombia dropped from 3rd place to 5th. Finally, Italy and Spain were replaced by Germany and Australia in the top 5 rankings.

Now, let's delve into the MITRE ATT&CK techniques associated with the alerts seen most frequently by customers in these countries.

United States

ID	Technique name	Tactic name	%
T1565	Data Manipulation	Impact	47.91%
T1071	Application Layer Protocol	Command and Control	15.32%
T1095	Non-Application Layer Protocol	Command and Control	15.32%
T1498	Network Denial of Service	Impact	7.02%
T0841	Network Service Scanning	Discovery	5.54%

The top threat techniques reported in U.S. customer environments reflect the top global techniques in the same descending order but in slightly different proportions.

Sweden

ID	Technique name	Tactic name	%
T1498	Network Denial of Service	Impact	34.13%
T1565	Data manipulation	Impact	28.77%
T1557	Adversary-in-the-Middle	Credential access; Collection	11.60%
T0841	Network Service Scanning	Discovery	4.82%
T0846	Remote System Discovery	Discovery	4.82%

Germany

ID	Technique name	Tactic name	%
T0841	Network Service Scanning	Discovery	**36.10%**
T0846	Remote System Discovery	Discovery	**36.10%**
T1498	Network Denial of Service	Impact	**14.17%**
T1071	Application Layer Protocol	Command and Control	**2.98%**
T1095	Non-Application Layer Protocol	Command and Control	**2.98%**

Australia

ID	Technique name	Tactic name	%
T1498	Network Denial of Service	Impact	**23.38%**
T0841	Network Service Scanning	Discovery	**21.10%**
T0846	Remote System Discovery	Discovery	**21.10%**
T1557	Adversary-in-the-Middle	Credential access; Collection	**20.05%**
T1110	Brute Force	Credential access	**4.99%**

Colombia

ID	Technique name	Tactic name	%
T1498	Network Denial of Service	Impact	**86.13%**
T0841	Network Service Scanning	Discovery	**2.85%**
T0846	Remote System Discovery	Discovery	**2.85%**
T1557	Adversary-in-the-Middle	Credential access; Collection	**2.36%**
T1110	Brute Force	Credential access	**2.31%**

In Colombia, the proportion of the network DoS attacks is significantly higher than in other countries, contributing to a whopping 86+% of total attacks seen here.

The main takeaway here is that, like each industry, each country has its unique profile of most prevalent threats. Knowing and understanding what threats are actively occurring in your country enables security experts to focus on achieving maximum results with available resources.

4. Is Your Wireless Network Clean? A Security Hygiene Audit

4.1 The Unseen Risks of Industrial Wireless Environments

Industrial environments increasingly rely on wireless communications, from handheld IoT sensors to critical control systems. Yet, most asset owners are unaware of the sheer number of devices communicating over the air within their facilities. This lack of visibility creates significant blind spots in security, leaving organizations vulnerable to threats that exploit unmonitored wireless networks.

Wireless networks, particularly in industrial environments, often operate outside traditional IT controls. Devices can communicate on legacy protocols or unsecured channels, making them attractive targets for attackers. One of the most underestimated challenges in wireless security is the difficulty of understanding which devices are active, what protocols they are using and how vulnerable these communications might be.

Without comprehensive monitoring, it is nearly impossible to know whether your wireless network truly secure.

4.2 Common Threats Targeting Wireless Networks

Wireless vulnerabilities can manifest in a variety of ways, often due to the inherent open nature of radio-frequency communications. Unlike wired networks, wireless networks rely on the transmission of signals through the air, making them more susceptible to interception and unauthorized access. This open communication channel provides ample opportunity for attackers to exploit weaknesses, often without leaving a trace. As industries increasingly rely on wireless technologies for critical operations, the need to identify and address these vulnerabilities has never been more urgent.

Below are some of the most common threats faced by industrial wireless environments:

- **Deauthentication Attacks** exploit weaknesses in network protocols to force devices off the network, disrupting operations and potentially paving the way for further attacks. They leverage a built-in feature in the Wi-Fi protocol, specifically in the management frames used for communication between devices and access points. By transmitting fake deauthentication frames, attackers can force devices to disconnect from the network. This can escalate into more severe disruptions, such as data interception and unauthorized access, especially when combined with additional malicious actions.
- **Rogue Access Points (APs)** can be deployed by attackers to impersonate legitimate networks, tricking devices into connecting and exposing sensitive data.
- **Eavesdropping** can occur when communications over unencrypted wireless protocols are intercepted, enabling attackers to steal credentials, read sensitive data or monitor operations. This threat is especially common over free, public Wi-Fi services in airports, hotels, etc.

- **Jamming Attacks** occur when malicious actors disrupt communications by overwhelming wireless channels, leading to downtime or operational inefficiencies.

In addition to traditional wireless vulnerabilities, Unauthorized UAV (Drone) Overflight has emerged as a growing concern, particularly in industrial environments. Drones, equipped with advanced communication technologies, can pose significant risks, including:

- **Signal Interception and Espionage:** Drones can fly over facilities, intercepting unencrypted wireless communications. This allows attackers to eavesdrop on sensitive data, such as proprietary designs, operational information, and control signals. In addition to intercepting signals, drones can be equipped with digital cameras to conduct visual surveillance, capturing images or videos of physical infrastructure, sensitive equipment, or areas that may otherwise be restricted. This form of espionage enables attackers to gather critical intelligence about a facility's operations, weaknesses, or security measures, potentially leading to the theft of intellectual property, strategic plans, or access to vulnerable systems.
- **Signal Jamming:** Drones can intentionally interfere with wireless communications by emitting strong signals on the same frequencies as those used by the targeted network. This type of attack can disrupt network operations, leading to temporary or prolonged downtime and potentially compromising the integrity of critical processes.
- **Network Access Attempts:** Some drones are equipped with technologies designed to exploit weaknesses in wireless networks. These drones may attempt to connect to unsecured or poorly protected networks, creating an entry point for cyber attackers to gain access to industrial control systems, allowing for further exploitation or manipulation.

The growing accessibility and capability of drones make this form of attack particularly dangerous, as they can operate covertly, monitoring or disrupting operations without detection. When combined with espionage capabilities, drones present a serious and evolving risk to industrial wireless security.

The common wireless threats described here are particularly alarming in industrial environments, where the consequences extend beyond data breaches to include operational disruption, safety risks and regulatory non-compliance.

4.3 Unprotected Wireless Networks Are Vulnerable to Deauthentication

Recent research performed by Nozomi Networks into wireless security uncovered widespread vulnerability of wireless networks to deauthentication attacks.

Our most concerning finding is that only 6% of observed wireless networks today are adequately protected against deauthentication attacks, as they lack Management Frame Protection (MFP), a crucial security feature designed to prevent attackers from spoofing management frames. In other words, the vast majority of wireless networks, including those in mission-critical environments, remain highly exposed to these kinds of attacks. In healthcare, for example, vulnerabilities in wireless networks could lead to unauthorized access to patient data or interference with critical systems. Similarly, in industrial environments, these attacks could disrupt automated processes, halt production lines or create safety hazards for workers.

4.4 Wireless Network Managed Frame Protection Status

Mitigation Steps Against Deauthentication Attacks

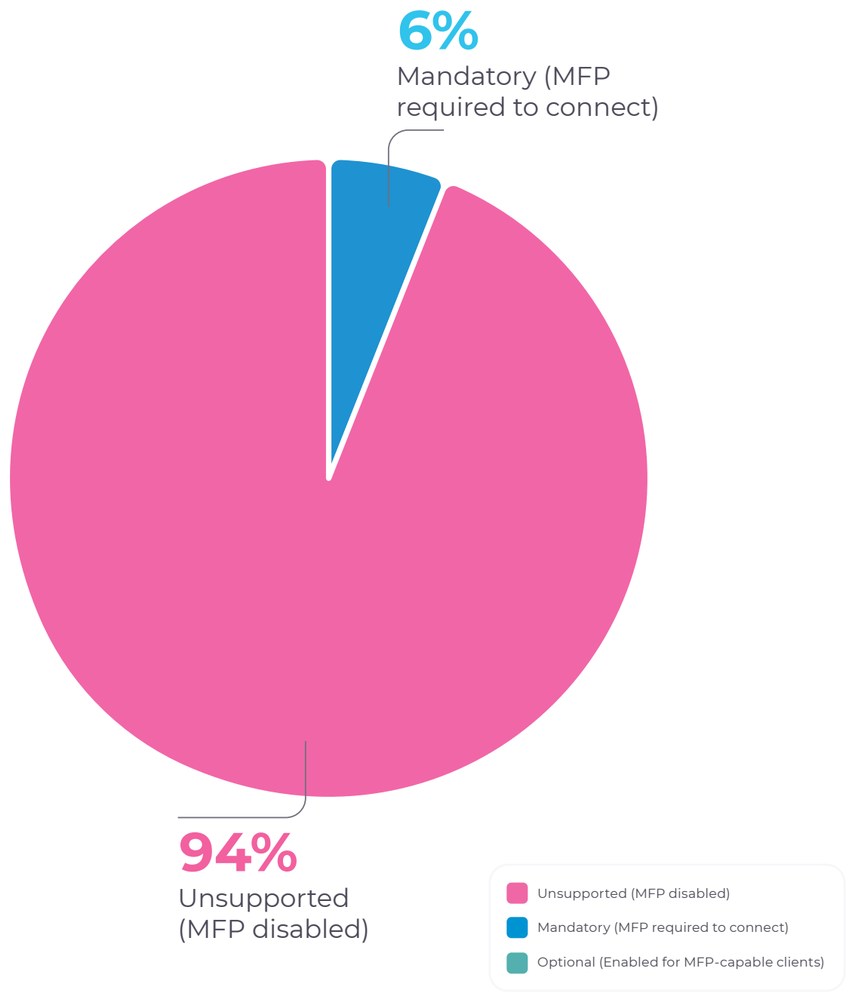
To protect against deauthentication attacks and improve wireless network security, organizations can take these immediate actions:

1. **Enable 802.11w (MFP)**, which is essential for defending against deauthentication attacks. This standard adds encryption to management frames, making it significantly harder for attackers to forge deauthentication messages and disrupt the network.
2. **Upgrade to WPA3**, which provides enhanced security features, including Protected Management Frames (PMFs). This protocol helps to protect against deauthentication attacks and ensures a more robust defense against wireless threats.
3. **Regularly monitor wireless networks** for signs of suspicious activity. By scanning for devices conducting deauthentication attacks or other disruptive behaviors, organizations can quickly identify and respond to threats.

4.5 Protecting Critical Infrastructure for Operational Continuity

As a generic guideline, monitoring wireless networks provides the visibility needed to detect unauthorized devices, identify vulnerabilities and protect against attacks in real time. By using wireless security technologies, organizations can continuously monitor the frequencies used by their wireless networks, gaining insights into the devices present, the security posture of the network and any potential threats. This proactive approach is key for detecting attacks before they can escalate into more serious incidents.

802.11w MFP Configuration Status Across Observed Wi-Fi Networks



Real-time monitoring also enables organizations to react swiftly to ongoing threats, minimizing the impact of attacks like deauthentication or other forms of signal disruption. Additionally, by continuously scanning the air, organizations can ensure that any unauthorized access points or rogue devices are identified and removed, reducing the likelihood of further compromise.

Ultimately, the importance of monitoring wireless networks cannot be overstated. As the number of wireless devices and connected systems grows, so too does the potential attack surface. By implementing comprehensive monitoring solutions and ensuring that wireless networks are properly secured, asset owners can protect their devices, ensure business continuity and safeguard sensitive information from potential cyber threats.

The solution begins with awareness. By deploying technology capable of scanning wireless frequencies and extracting telemetry, asset owners can achieve unprecedented insight into their environments. Telemetry collected includes device identities, communication protocols, and vulnerability assessments, enabling proactive defenses against potential threats.

5. Navigating Device Vulnerability Trends: Key Stats for Security Strategy

In this section we review all ICS advisories released during the second half of 2024, identifying new trends and highlighting changes. During this period (July 1 – December 31), CISA released 241 advisories, with 619 vulnerabilities affecting products from approximately 70 vendors. Here's a closer look at these vulnerabilities.

If you're a Nozomi Networks customer, you are covered for these vulnerabilities because asset intelligence, including CVEs, is baked into our product by the Nozomi Networks Labs.

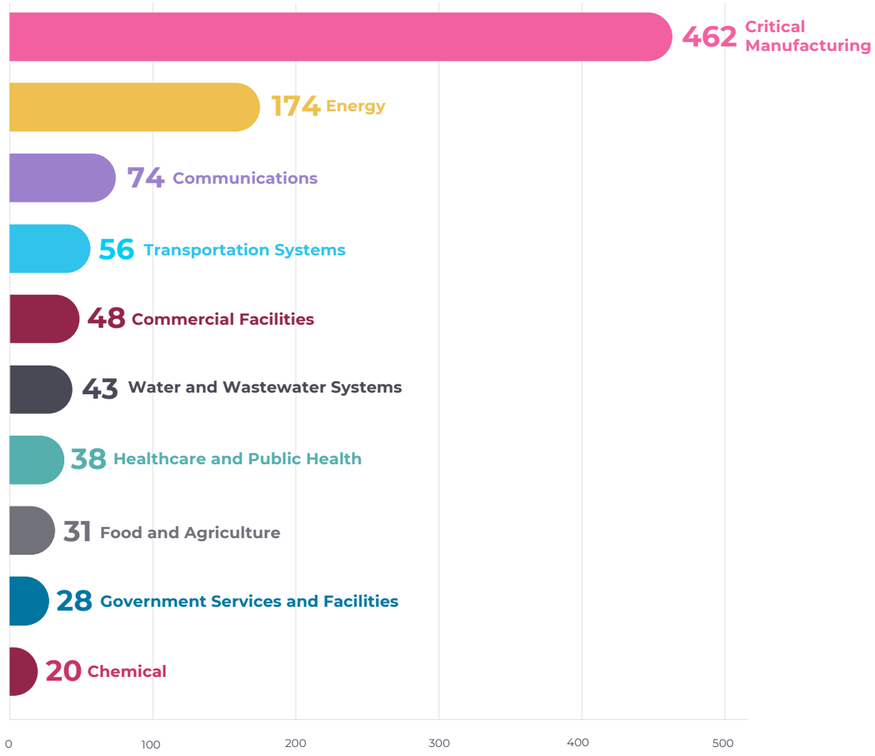
5.1 Number of CVEs Released by Sector

The chart on the right identifies the top 10 industries affected by the vulnerabilities highlighted in the ICS advisories during this period.

As with the previous six-month period, the Critical Manufacturing and Energy sectors lead the chart. Most notably, the Communications sector jumped onto the list in 3rd place, possibly tied to Salt Typhoon targeting telecommunications companies during this period. Increased scrutiny of exploitable vulnerabilities may have led researchers to discover and report more CVEs. The emergence of the Communications sector on the list displaced perennially targeted sectors such as Transportation, Commercial Facilities and Water and Wastewater Systems by one position each. Given the importance of communications systems in our daily lives, we will closely monitor

Top 10 Sectors by Number or ICS CVE Advisories

July 1 to December 31, 2024



vulnerabilities associated with this sector to help ensure our customers are protected.

The rise of vulnerabilities affecting Government Services and Facilities is another highlight from this period, after the sector dropped off the list in the first half of 2024. Nozomi Networks is proud to take part in multiple initiatives around the globe aiming to improve the cybersecurity posture of government organizations at various levels.

5.2 Number of CWEs Associated with CVEs

Now, let's turn to the top Common Weakness Enumeration (CWE) categories associated with these vulnerabilities.

The universal Improper Input Validation CWE once again takes first place, reminding us how important input sanitization is. As in the previous reporting period, it is followed in close succession by the **Out-of-Bounds Write** and **Out-of-Bounds Read**. CWEs **Path Traversal** and **Uncontrolled Resource Consumptions** also reappear, albeit in slightly different positions. The recurrence of these familiar CWEs reinforces the need to integrate the best available OT/ICS-specific threat intelligence into your cybersecurity platform to ensure you can automatically detect known issues in your environment.

Top 10 CWEs Associated With ICS Advisories

July 1 to December 31, 2024

5.3 Risk Score Statistics

Where available, we also looked at the Common Vulnerability Scoring System CVSS (v4 where available, otherwise v3) and Exploit Prediction Scoring System (EPSS) risk scores assigned to the top ICS vulnerabilities reported during this period. Here's what we found:

- Four vulnerabilities were marked as Known Exploited Vulnerabilities (KEVs), meaning they have been observed as actively exploited in the wild.
- 20 vulnerabilities have an EPSS score indicating a >1% probability of being exploited in the wild. This threshold is generally considered high.
- The average CVSS risk score was 7.43.
  - ~71% of vulnerabilities received a High or Critical risk score (≥7.0).
- The average EPSS score was 0.012.

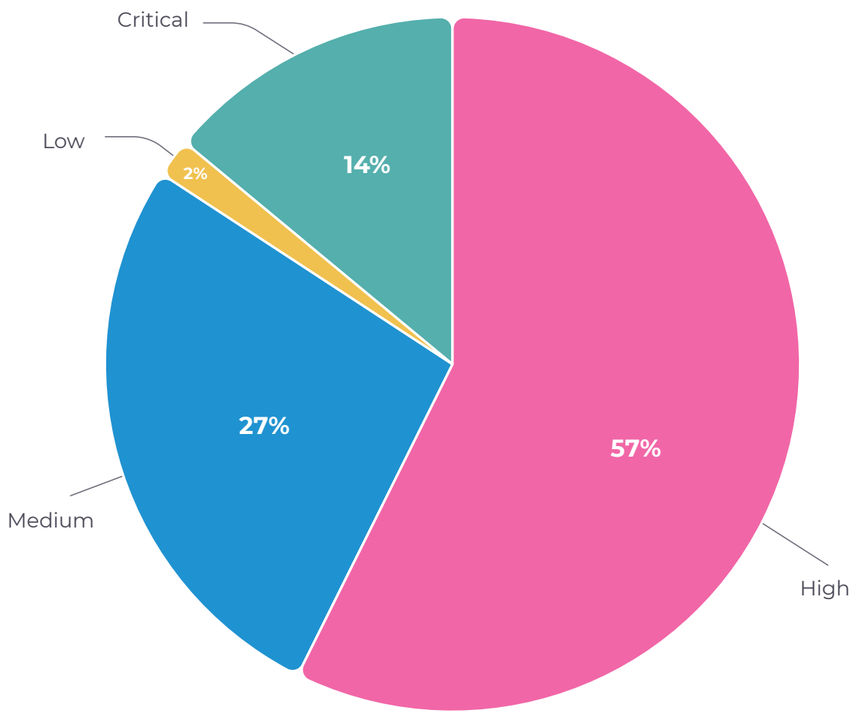
The identification of four Known Exploited Vulnerabilities (KEVs) is significant because it highlights vulnerabilities that are actively being targeted by threat actors, emphasizing the need for immediate mitigation. Similarly, the 20 vulnerabilities with the EPSS score above 1% underscores their high likelihood of exploitation, signaling a crucial area of focus for proactive risk management.

As we can see, the CVSS risk scores for vulnerabilities affecting OT are generally high, emphasizing the need for organizations to resolve them promptly. High EPSS scores and the KEV flag are excellent indicators for prioritization. While the total number of vulnerabilities flagged this way remains relatively low, these are generally the most critical vulnerabilities to address first.

To handle vulnerabilities efficiently, organizations should also adopt metrics tailored to their unique environments — such as the criticality of individual assets — to make more informed prioritization decisions and ensure risk scores reflect how your organization assigns risk.

Distribution of Vulnerabilities by CVSS Risk Score*

July 1 to December 31, 2024



*Where available

6. The Botnet Epidemic: Statistics, Threats, and Defenses

In this section, we explore the world of IoT botnets, examining their mechanics, the threats they pose to cybersecurity and effective strategies to combat this growing threat. All data is collected by our globally distributed chain of honeypots, completely unrelated to our customers' environments. From this vantage point, we analyze the tactics, techniques and procedures currently employed by botnets to help asset owners better protect their systems and more quickly spot anomalies

If you're a Nozomi Networks customer, you are covered for these IoT threats because intelligence regarding them is baked into our product by the Labs team.

6.1 Attack Source Locations

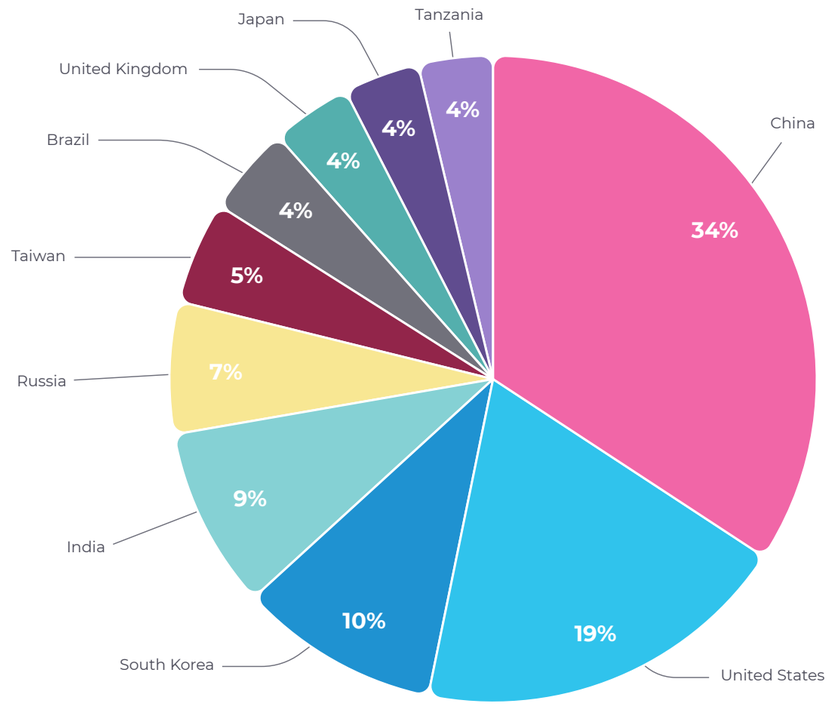
This chart represents the distribution IoT botnet attacks on our honeypots during the second half of 2024, based on absolute number of attacks from each country of origin. Typically, the attacks come from compromised devices.

Note that the countries with the largest shares of the pie chart don't necessarily have weaker cybersecurity postures. On the contrary, countries with high levels of automation typically have more smart devices that may be compromised and become part of a botnet.

As in several previous periods, most of the attacks came from China and the U.S. That's expected given the size and the level of automation in the two most dominant countries

Distribution of Attacks Based on IP Address Origin

July 1 to December 31, 2024



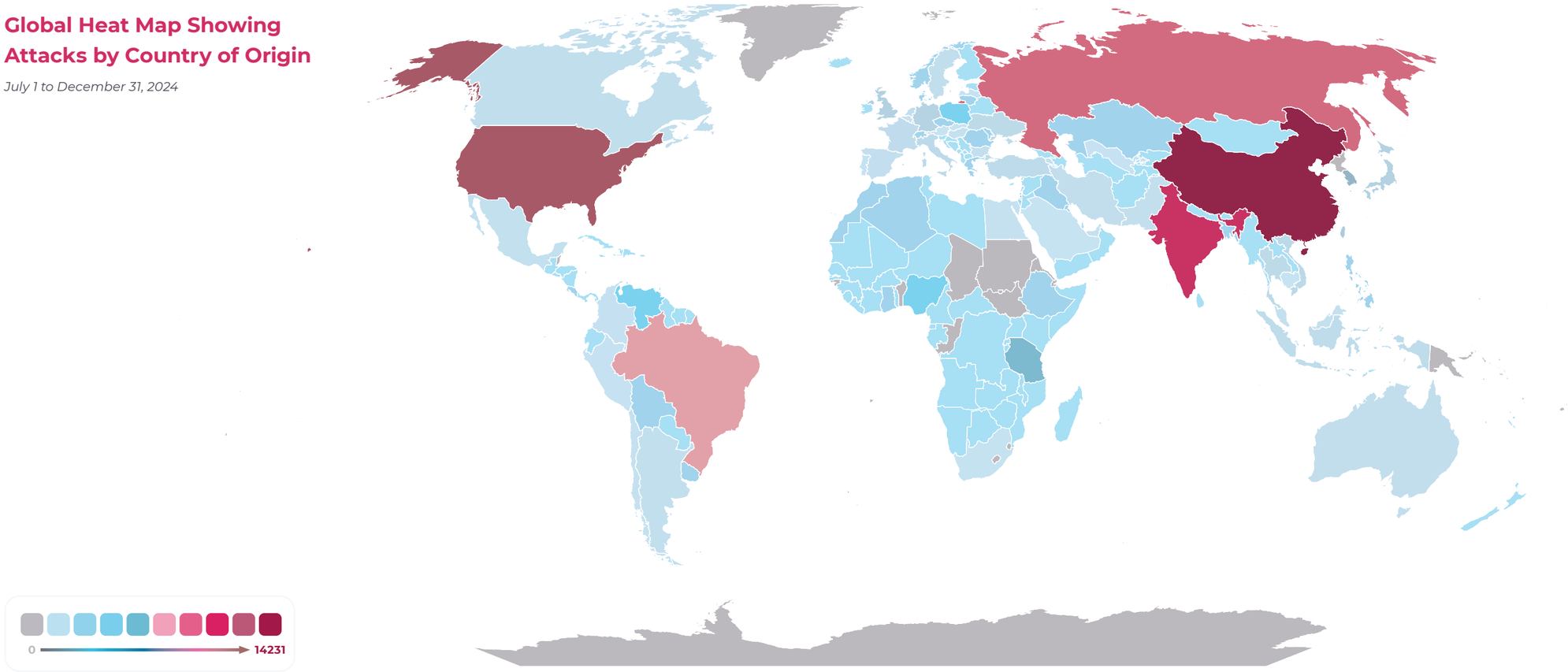
in the world. Comparing the remaining rankings to the first half of 2024, South Korea and India swapped positions to take 3rd and 4th place respectively. Russia and Taiwan moved up to overtake Brazil and Japan from 7th and 8th position to 5th and 6th.

Finally, Singapore fell out top 10 chart and was replaced by Tanzania.

Keeping an eye on global activity helps the Nozomi Networks Labs team stay on top of big emerging botnets. This work provides the flow of indicators of compromise (IoCs) coming from our honeypots and signatures we create based on collected samples, which are funneled to our customers via the Threat Intelligence subscription.

Global Heat Map Showing Attacks by Country of Origin

July 1 to December 31, 2024



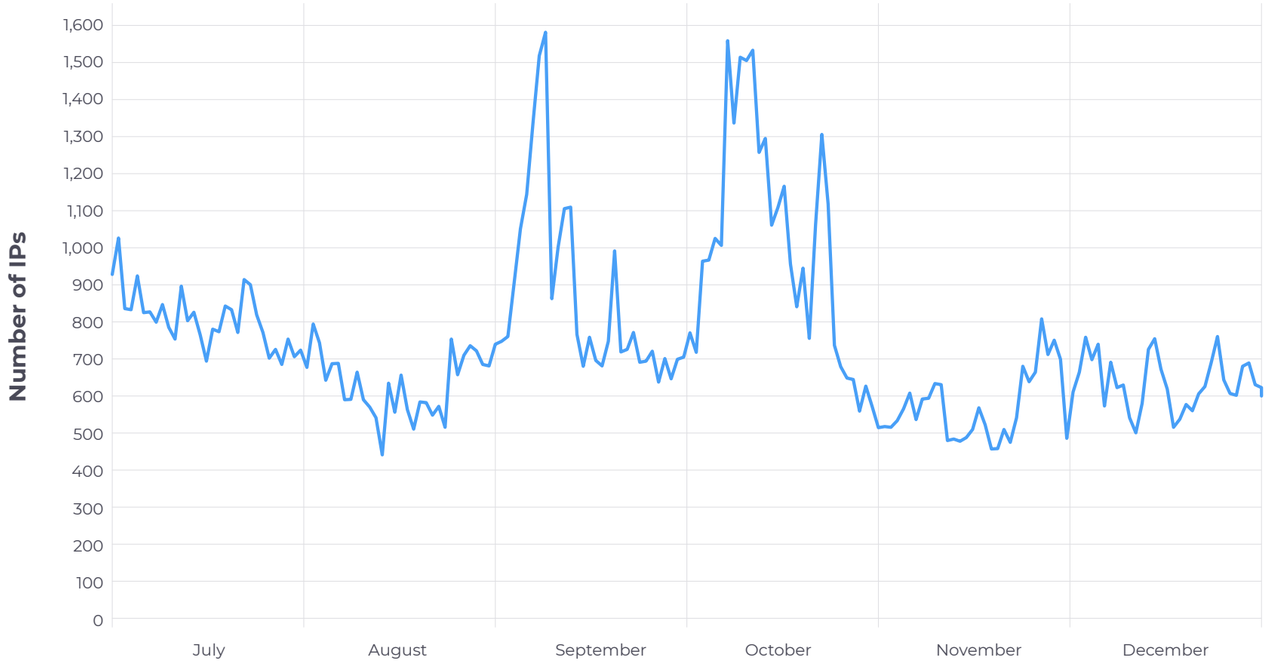
6.2 Number of Unique Daily Attacker IPs

We also graphed the daily activity of IoT botnets with unique IP addresses that initiated attacks on our honeypots in the last six months of 2024. As usual, big spikes may represent the emergence of new botnets or upgrades to existing ones, while big dips may signify the botnet deactivation or takedown. Here, for example, we can see that the highest spikes were recorded at the beginning of September and October. On those days, we collected the highest number of unique new IP addresses (peaking at 1,595 in early September), which enabled us to promptly notify to our customers of this activity through our Threat Intelligence feed.

The peak number of simultaneous attacks for this period is more than 1.5 times greater than during the previous period (roughly 1,600 vs. 1,000). The average number of daily attacks initiated from unique machines was similarly higher, (758 vs. 566), signifying that the botnets were significantly more active during this period. We will continue keeping a close eye on these trends to protect customers from emerging threats before they can cause damage.

Daily Volume and Activity from Unique Attacker IP Addresses

July 1 to December 31, 2024



6.3 Top Credentials Used

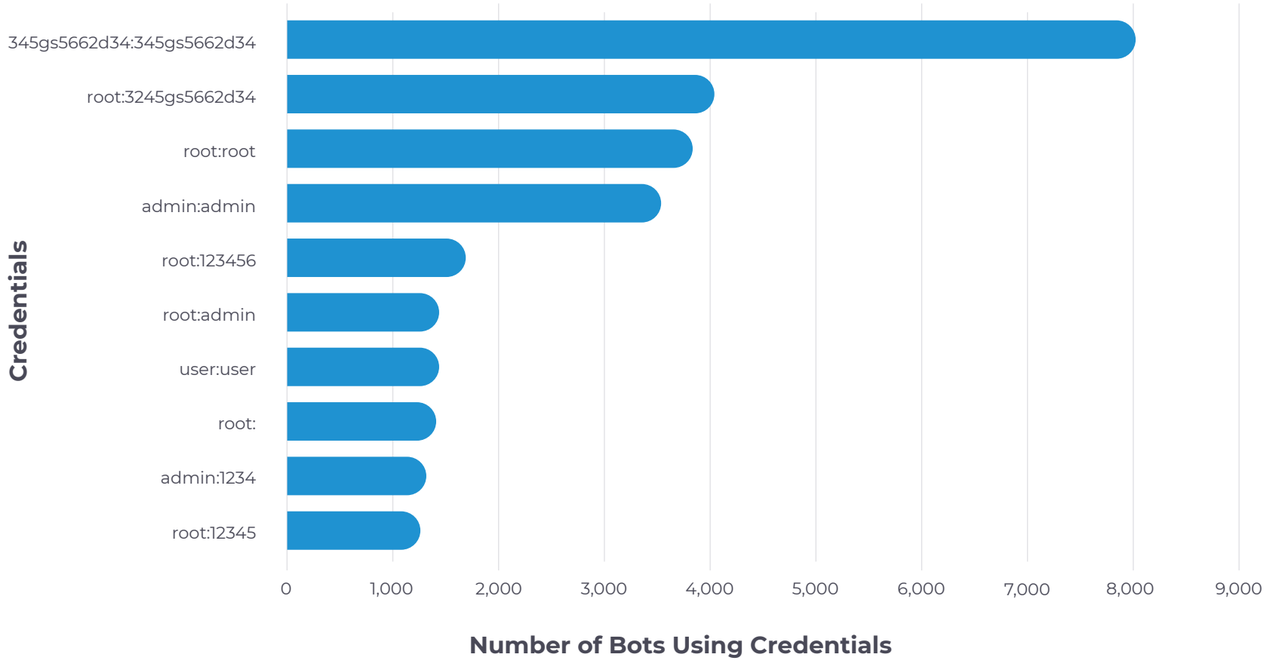
Brute-forcing SSH and Telnet credentials remains one of the most popular options for attackers to establish initial access to the vulnerable devices. In this section, we see the top credentials used by botnets in the last six months of 2024. The X axis indicates the total number of unique IP addresses that used the credentials to initiate an attack.

Based on the frequency of **root** and **admin** in the credential pairs, it's clear that attackers favor using credentials that will grant them high privileges and enable better persistence on the compromised device. This is yet another stark reminder that basic cyber hygiene is critical. It's impossible to overstate the importance of following strong credential management practices, beginning with promptly identifying and changing default credentials in *all* devices — OT, IT and IoT. That includes changing default embedded credentials, especially if they are highlighted in this list.

Nozomi Networks products use various ways to detect and notify customers about weak credentials being used in their environments so they can be changed.

Top Credentials Used by Attackers for Initial Access to Honeypots

July 1 to December 31, 2024



6.4 Top Executed Commands

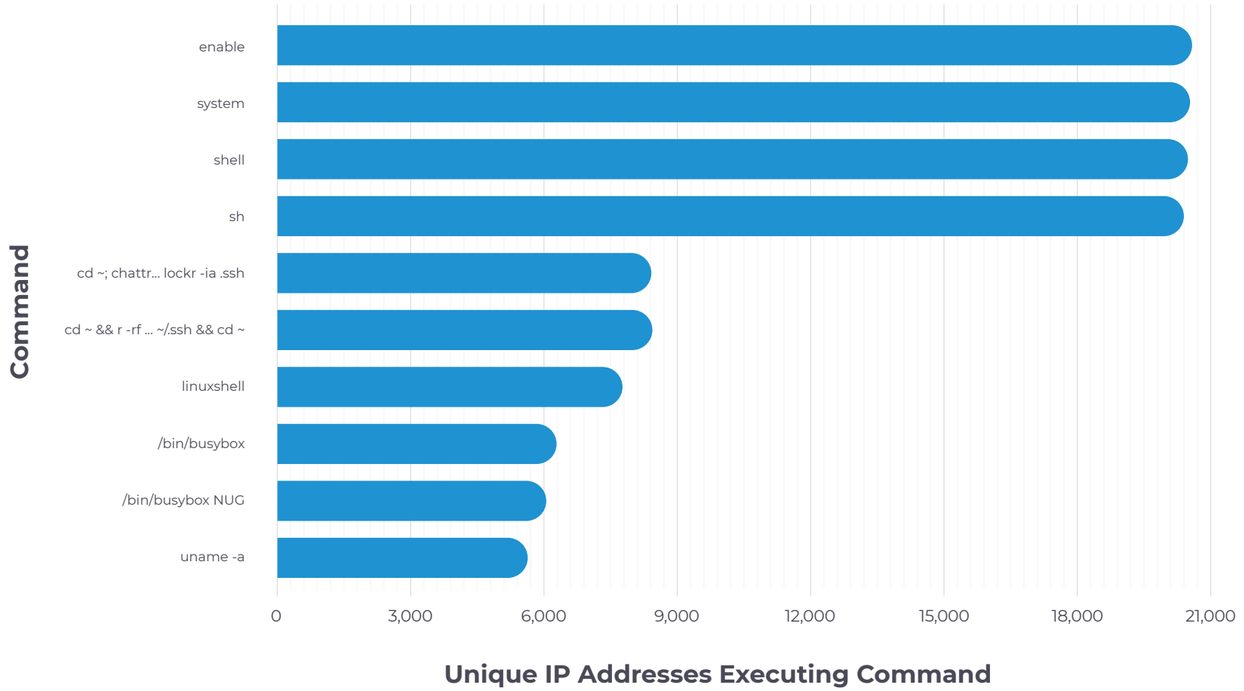
Once attackers believe they've established initial access to our honeypots, they execute various commands to continue the attack. Here are the most popular commands. Once again, the numbers on the X axis are the total number of unique IP addresses that executed the commands.

Apart from the universal commands needed to establish the right shell environment (**enable**, **system**, **shell**, **sh**, **linuxshell** or **busybox**) that we typically see, three other frequently executed commands stand out:

- `"cd ~; chattr -ia .ssh; lockr -ia .ssh"`[2] will manipulate the **.ssh** directory under the current home directory to make it easily editable. This directory stores public keys allowing future easy access to the compromised system. Don't be confused by the "lockr" tool here; in this case the attackers previously copied the standard chattr tool under this name, which explains why the arguments are the same for both tools.
- `"cd ~ && rm -rf .ssh && mkdir .ssh && echo ""ssh-rsa AAAA<redacted> mdrfckr"">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~"`[3] will delete all the previous public SSH keys and add a new public key belonging to the attackers to ensure that only they can now connect to the compromised system via SSH.
- `"uname -a"` will collect basic information about the compromised system.

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

July 1 to December 31, 2024



[2] Non-truncated command: cd ~; chattr -ia .ssh; lockr -ia .ssh
[3] Non-truncated command: cd ~ && rm -rf .ssh && mkdir .ssh && echo ""ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUh BGE7VvAcwdli2a8dbnrTOrbMzl+5O73fcBOOnvNoaJe0QXxzilg9eLBHpgLMuakb5+BgTFB+rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvc EmPecjdySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCGPK5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14u jvcD9iUKQTTWYYjIlu5PmUux5bsZ0R4WFwdIe6+i6rBLAsPKgAySVKPRK+oRw== mdrfckr"">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~

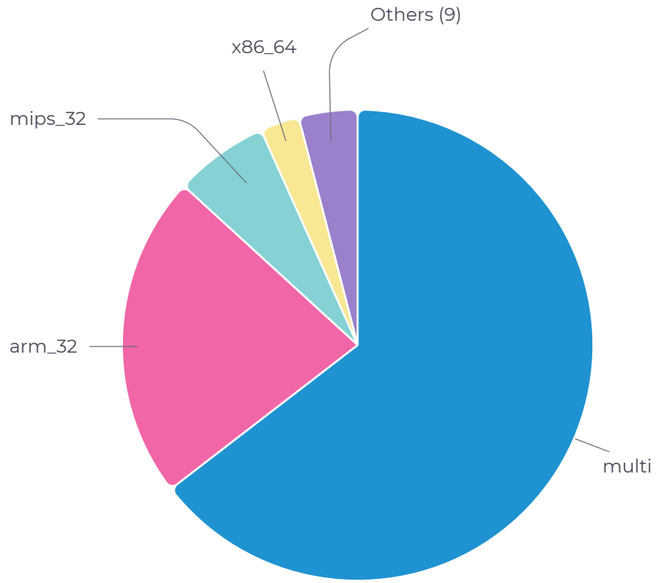
6.5 Top Payload File Types

Next, we looked at what second-stage payloads were delivered to the compromised machines once initial access was established.

As usual, most of the payloads comprised various types of scripts supported by multiple architectures (multi). Regarding executable payloads, 32-bit ARM payloads are still the top choice of the attackers, followed by 32-bit MIPS. An important takeaway is that your cybersecurity solution should provide protection against executables targeting various architectures, not only the most common ones like ARM and x86.

Top Payload Types by Targeted Architecture

July 1 to December 31, 2024



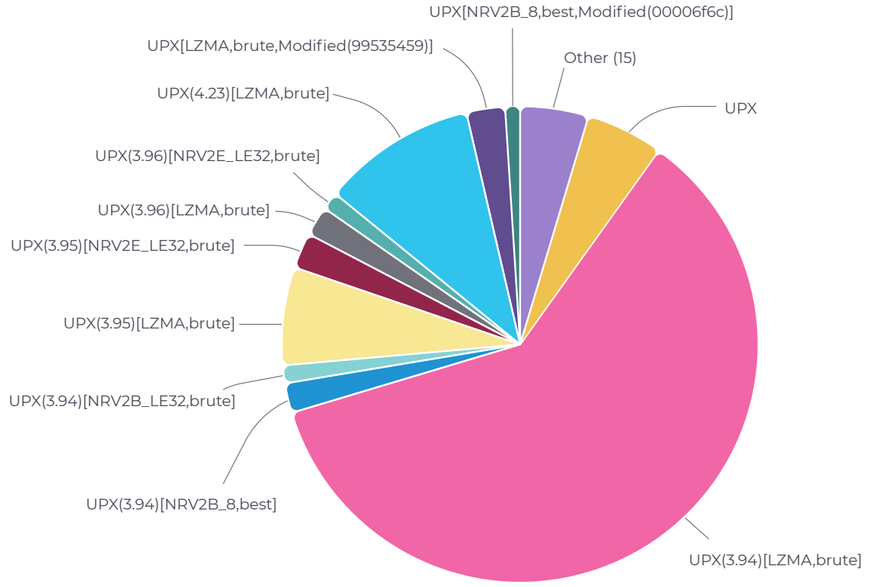
6.6 Top Payload Packers

To proactively protect yourself from modern threats, it's crucial to ensure that your cybersecurity solution can detect malware that has been packed, a common compression technique threat actors use to protect their payloads from being detected and analyzed. The distribution of payload packer looks very much the same across the first and second half In the second half of 2024. Once again, UPX in its many versions is the top choice of attackers.

As we can see, old versions of UPX, especially 3.94, remain the most used despite the availability of more recent versions for many years. However, we expect new open-source packers that support ELF files like kiteshield will gain popularity and start ranking here.

Top Payload Types by Targeted Architecture

July 1 to December 31, 2024



7. Insights Into the Latest OT Malware

OT systems form the backbone of critical infrastructure — from power grids to manufacturing plants — and sophisticated OT-targeted malware is an ever-evolving threat. As cybercriminals refine their tactics, these systems face unprecedented risks that can disrupt operations, jeopardize safety and even threaten economic stability.

In the past six months, attackers have developed new OT malware tools such as BUSTLEBERM and OrpaCrab. Continuous monitoring, rapid detection and adaptive defenses are not just best practices — they're imperatives to protect your environment. Staying ahead of malicious actors requires more than reacting to incidents; it demands constant vigilance and a commitment to evolving with the constantly changing landscape to anticipate change.

7.1 BUSTLEBERM aka FrostyGoop

The emergence of BUSTLEBERM (aka FrostyGoop) malware, reportedly used as a cyberweapon to cut energy in Ukraine, once again highlights the importance of continuous threat monitoring to safeguard critical infrastructure. This malware was engineered to misuse the standard functionality of the Modbus protocol to damage systems that oversee industrial processes in energy and other sectors. Essentially, it's a command line tool that allows attackers to send arbitrary legitimate commands to the OT hardware. This simplicity makes it dangerous precisely because it lacks artifacts commonly found in malware, such as anti-reverse engineering techniques.

The day after this threat was made public, Nozomi Networks analysts published **our own research**, including YARA rules. In addition, our partner Mandiant already had indicators of compromise (IoCs) for it, which are available to our customers through the Nozomi Threat Intelligence Expansion Pack, powered by Mandiant.

NOZOMI NETWORKS BLOG

Cyberwarfare Targeting OT: Protecting Against FrostyGoop/BUSTLEBERM Malware for Cybersecurity

On July 23, 2024, the new OT malware called FrostyGoop aka BUSTLEBERM became known to the general public. Linked to the ongoing war in Ukraine, where according to third-party reports, it was used as a cyber weapon to disrupt critical infrastructure.

Read More ›

7.2 OrpaCrab aka IOCONTROL

First documented by QiAnXin XLab, OrpaCrab aka IOCONTROL malware was **linked to Iranian actors targeting IoT and OT environments** in the U.S. and Israel. This malware is designed to infiltrate devices such as cameras and routers in IoT, and PLCs and HMIs in OT. Its modular structure allows it to operate across various platforms. Notably, IOCONTROL uses unorthodox approaches such as MQTT and DNS-over-HTTPS (DoH) for network communications. Upon initial discovery of OrpaCrab by QiAnXin Xlab, Nozomi Networks quickly shipped protection against this threat to customers, even before more insights became public.

7.3 Ransomware in OT

While ransomware is not traditionally considered an OT threat, its ability to disrupt IT environments that are closely integrated with OT systems makes it a significant risk to critical infrastructure. Modern industrial environments rely on a seamless connection between IT and OT systems for data sharing, operational efficiency and process optimization. Ransomware attacks on IT networks can cause cascading effects, such as halting OT operations, disrupting production lines or even compromising safety systems. This interconnectedness means that OT environments are indirectly exposed to the dangers of ransomware, making it essential for OT cybersecurity companies to incorporate ransomware mitigation strategies into their defenses. In December 2024 alone, our products raised 268 alerts associated with ransomware deployment attempts across all our customers submitting anonymized telemetry.

The ripple effects of ransomware can be just as devastating as a direct OT-targeted attack. A ransomware-induced IT outage can paralyze operational processes, delay recovery timelines and expose organizations to significant financial and reputational damage. Moreover, as ransomware tactics evolve to include data exfiltration and targeted attacks on industrial environments, the lines between IT and OT threats are becoming increasingly blurred. To safeguard OT environments, companies must prioritize endpoint protection, network segmentation and real-time monitoring to detect ransomware threats early and minimize their potential impact on critical infrastructure. By addressing ransomware as a core risk, OT cybersecurity companies can enhance the overall resilience of industrial systems.

IN DECEMBER 2024

268

alerts associated with ransomware deployment attempts raised by our products

8. 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.

8.1 Implement a risk reduction strategy

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. In addition, signature-based detections may not be enough to protect against new threats. It's important to embrace a layered approach and adopt solutions that can detect anomalous behavior based on your established baseline.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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

NN-SEC-RP-FULL-2024-2H-001