NOZOMI NETWORKS LABS

REPORT

OT/IoT Cybersecurity Trends and Insights

2024 1H Review | July 2024

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 Introduction

Regulatory pressures around the globe are requiring CISOs and corporate boards to assume greater accountability for enterprise-wide cybersecurity, including operational technology (OT), industrial control systems (ICS) and Internet of Things (IoT) devices. In the U.S., the Securities and Exchange Commission now requires public companies to disclose information on “material” breaches and document their overall risk management, strategy and governance framework. Such regulatory pressure, coupled with rising cyber insurance costs and coverage restrictions, may be the forcing function needed for companies to adopt holistic strategies.

These are well-known challenges, however. CISOs are assuming responsibility for security domains they know little about that require different tools and methods. Bringing OT and IoT security into the enterprise fold means CISOs must also overcome cultural silos between InfoSec and OT engineering teams that have impeded efforts to secure the expanding attack surface. Meanwhile, OT software and hardware vulnerabilities continue to increase, threat actors are harnessing AI in an effort to stay ahead of defenders and the geopolitical climate is intensifying.

In this report, we look at the trends affecting OT and IoT cybersecurity for the first five months of 2024 and what they mean for InfoSec executives and owners/operators of critical infrastructure.

1.1 Key Findings

- **ICS CVEs:** CISA released 134 ICS advisories mentioning 842 vulnerabilities affecting products from 49 vendors.
- **Impacted industries:** Three of the top five industries affected by new ICS CVEs — Critical Manufacturing, Energy, and [Water and Wastewater]() — are sectors the U.S. and other governments are warning to be on the lookout for nation-state activity (such as [Volt Typhoon]()). Authorities are also stepping up cybersecurity oversight.
- **OT intrusion alerts:** Illegal parameters accounted for almost 20% of alerts, followed by three types of network anomalies and attacks: malformed traffic, TCP floods and network scans.
- **IoT botnet landscape:** Nearly half (46%) of botnet attacks monitored by Nozomi Networks honeypots originated from unique IP addresses in China, followed by the U.S. (16%). The top four executed commands after initial access were the shell commands `“enable”`, `“system”`, `“shell”` and `“sh”`. The vast majority of payloads were shell scripts not tied to any one architecture.

ICS CVEs STATS

134

New Advisories Reported by CISA

842

Total ICS-CERT Vulnerabilities Disclosed

49

Total Vendors Affected by Disclosed Vulnerabilities

INTRUSION ALERTS

Alert category	Percentage of all alerts
Illegal parameters request	19.79%
Malformed traffic	15.60%
TCP flood	7.15%
Network scan	6.41%

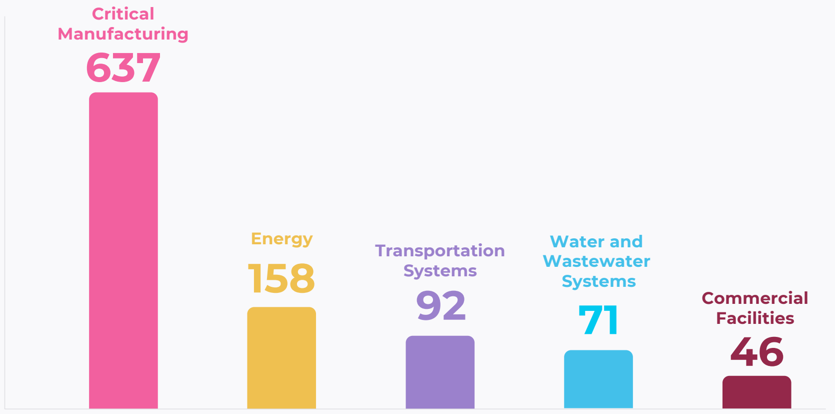
IT BOTNET LANDSCAPE

46% **Highest % of IoT botnet attacks originate in China**

16% **Next highest % originate in U.S.**

Top 5

Sectors Affected by Disclosed Vulnerabilities



1.2 The Rise of Nation-State Threats on OT

This report covers vulnerabilities, attacks and key cybersecurity indicators of events from the wild during the first half of 2024.

In parallel, nation-state threats have become more prominent due to rising global tensions, shifting from espionage to more destructive goals.

Traditional IT cybersecurity focuses on protecting sensitive data from theft. When dealing with nation-state actors, the primary concern is national security data. However, if the focus is on protecting financial or less critical data, priorities shift to mitigating ransomware, insider threats, data leaks and brand-tarnishing activities.

Nation-state threats come in two main forms: espionage and destruction.

These are particularly concerning for people managing critical infrastructure in OT environments. When these threats emerge, we must consider the complexity of attribution, which is rarely 100% certain. Even with some level of attribution, pinpointing the exact division responsible can be challenging.

For example, reports on Volt Typhoon indicate that Chinese threat actors are expanding their objectives beyond espionage to include potential sabotage and disruption of critical infrastructure. They operate globally, using open-source tools, black-market exploits, zero-day vulnerabilities, and living-off-the-land techniques that conceal their activities.

They are positioned within critical infrastructure with little to no espionage value and were only recently discovered in a multi-year effort.

Nation-state risks have also risen due to regional events including rising tensions, conflicts and full-blown wars. Recent public exposure of these events could shed light on unattributed activities reported historically over several years, across various tools.

While this report does not implicate specific nation state actors, these developments should be top of mind as the threat landscape evolves and new OT and IoT CVEs are released.

2 The Vulnerability Landscape

In this section we analyze data from all ICS advisories released by CISA between January 1 and May 30, 2024. During this period, CISA released 134 ICS advisories mentioning 842 vulnerabilities affecting products from 49 vendors.

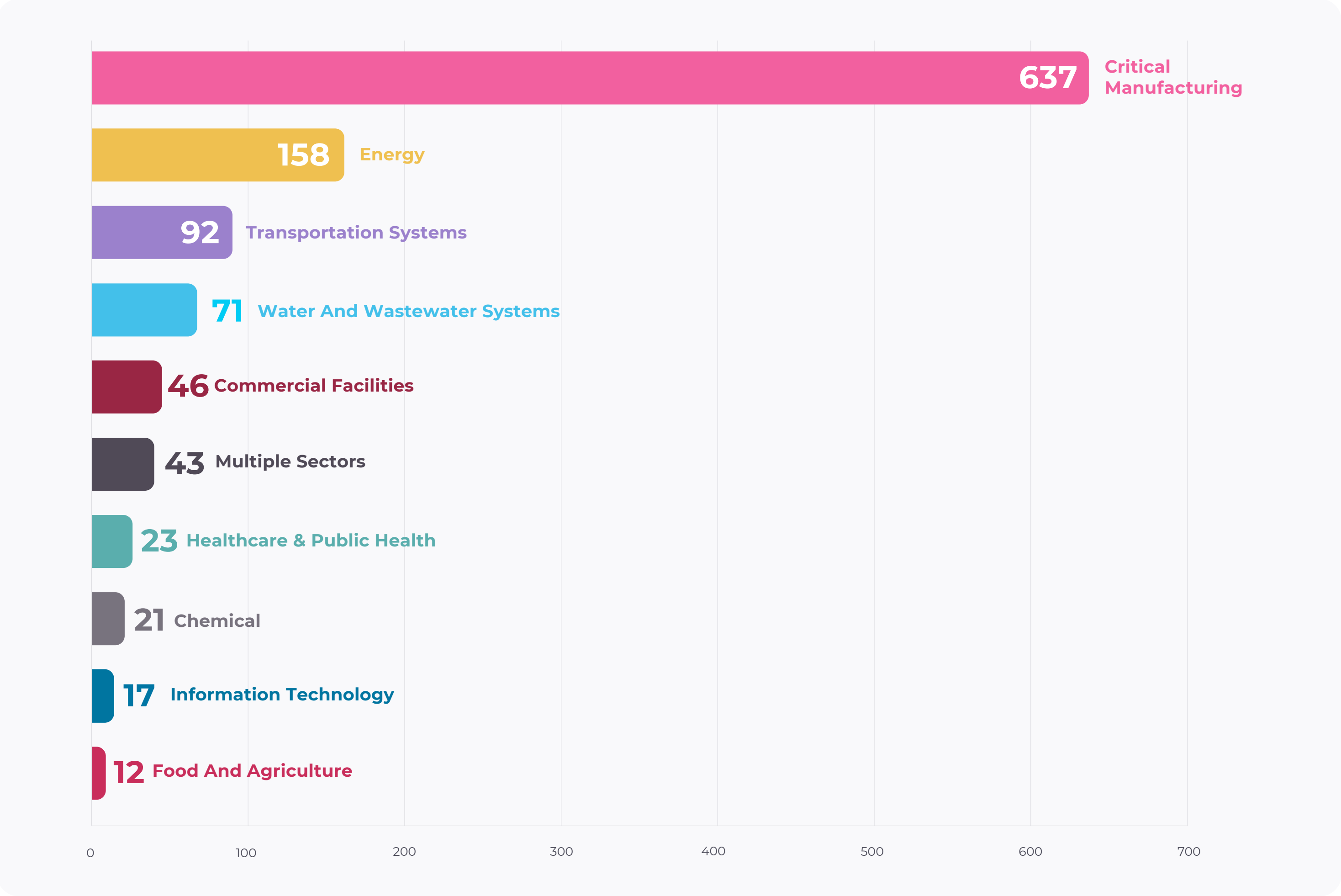
If you're a Nozomi Networks customer, you are covered for these vulnerabilities because asset intelligence, including CVEs, is baked into our product by the Labs team.

2.1 Number of CVEs Released by Sector

Looking at the top 10 industries affected by vulnerabilities, Critical Manufacturing was the most affected industry – the same as our previous reporting period. Manufacturing topped the list by a wide margin, with 479 more reported ICS CVEs than the next sector, Energy.

According to the ICS Advisory Project and Industrial Data Works' first annual **ICS Vulnerabilities report**, for calendar year 2023, these sectors were the most impacted by CISA ICS advisories, with Manufacturing and Energy respectively accounting for 44% and 20% of total reported ICS CVEs.

Water & Wastewater Systems and Commercial Facilities remained at #4 and #5. However, Transportation Systems leaped from ninth place to third, giving stakeholders in this **sprawling sector** reason to pay close attention to the advisories, including available remediation steps.

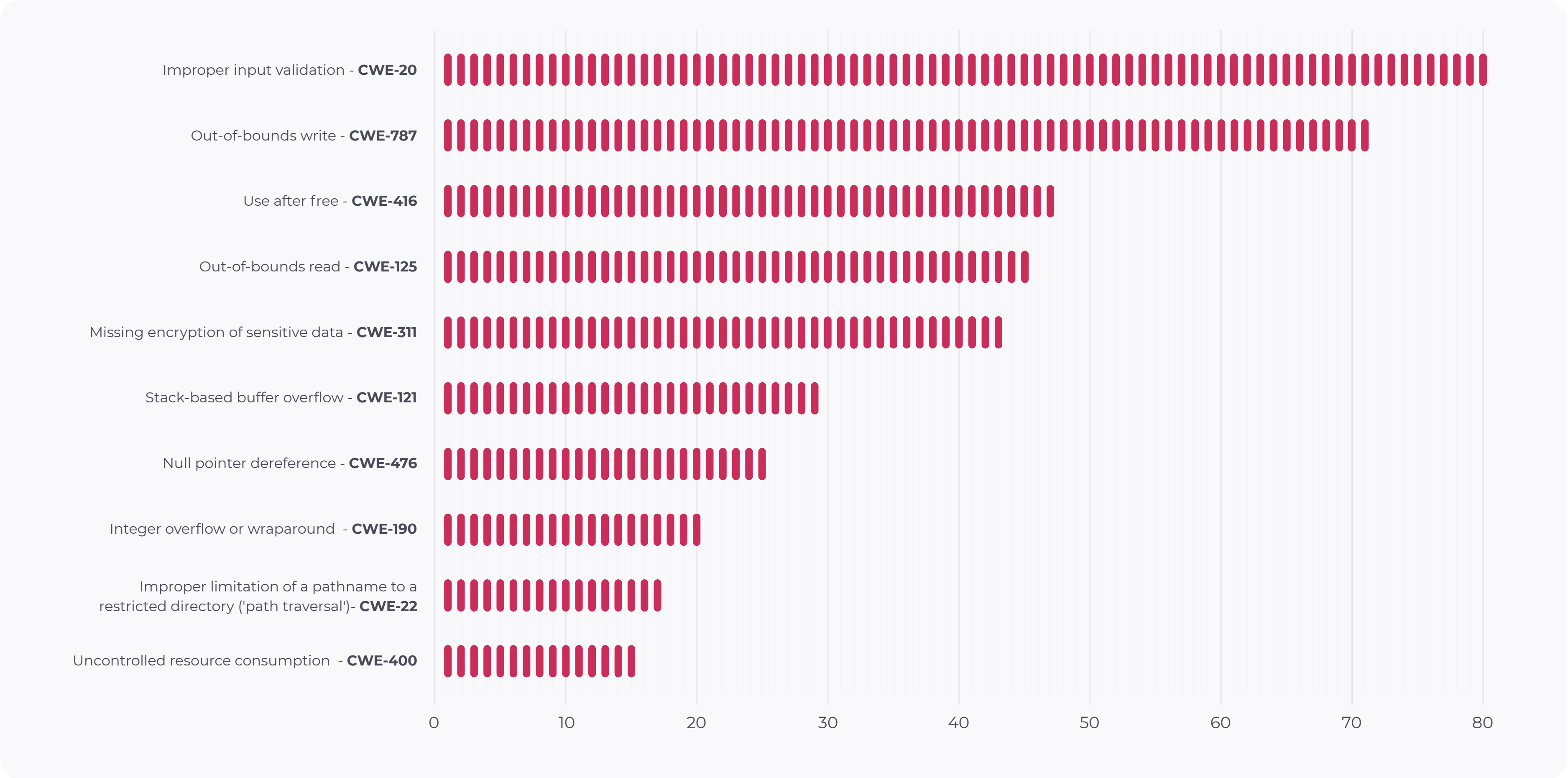


Top 10 industries with most reported vulnerabilities form January 1 to May 30, 2024.

2.2 Number of CWEs Associated with CVEs

Now let's take a closer look at the categories of the vulnerabilities mentioned in these latest ICS advisories. Comparing the distribution of Common Weakness Enumeration (CWE) categories for the first half of 2024 to the previous report, we can see some shuffling across the top four entries; IMPROPER INPUT VALIDATION, OUT-OF-BOUNDS READ and OUT-OF-BOUNDS WRITE (associated with incorrectly handling data in memory) and USE AFTER FREE. IMPROPER INPUT VALIDATION jumped from third place for the last half of 2023 to first place, with 27 more CWEs, reminding us how important it is to sanitize user input before processing it.

Shifts among the next three categories were minor, but MISSING ENCRYPTION OF SENSITIVE DATA jumped from #9 to #5 with more than double the number of CWEs (20 vs. 43), highlighting the importance of introducing proper encryption of the sensitive data at the right places.



Top 10 IDs associated with vulnerabilities reported from January 1 to May 30, 2024.

3

Attack Statistics from OT Environments

In this section, we analyze the telemetry collected by the Nozomi Networks monitoring platform, provided by customers participating in our anonymized-data sharing project.

Thanks to the customers who have opted in to securely share their data, we are able to aggregate detection data and provide unique insights into what types of threats were the most prevalent in real OT/IoT environments all over the world during the first half of 2024.

3.1 Top Critical Intrusion Alerts

In this section we look at the top 10 most critical types of intrusion alerts detected by Nozomi Networks products between January 1 and May 30, 2024, from the most to least detected.

Looking at the top 10 alerts, we see that common security issues like poor credential handling and brute-force attacks that produce alerts for **Cleartext passwords** (#6) and **Multiple Access Denied** events (#7), respectively, are still in the top 10 of the most common issues found in customer OT and IoT environments. Notably, **New link group** (#5) and **New link** (#8) alerts appear in the top 10 for the first time during this period. These alert types notify our customers about suspicious new connections that may indicate a potential compromise of associated assets.

Two technical notes on the data:

- To improve analysis and reduce the total volume of alerts, we consolidated multiple related attack patterns into single alerts. As a result, **Network scan** fell from #1 to #4. We also know that network scanning can be very noisy, commonly sending many different payloads to multiple devices and machines. Moreover, many companies actively scan their own environment to search for vulnerabilities, which is a best practice.
- **Missing variable request** alerts, which detect attackers potentially sending bogus requests to OT hardware, are the most common alert type raised among participating customers. However, because the logic of these alerts changed significantly in the middle of this reporting period, we decided to temporarily exclude it to avoid skewing the data.

Top 10 Most Critical Types of Intrusion Alerts

January 1 to May 30, 2024

Alert type	Alert category	Percentage
Illegal parameters request	OT Specific Threats	**19.79%**
Malformed traffic	Network Anomalies and Attacks	**15.60%**
TCP flood	Network Anomalies and Attacks	**7.15%**
Network scan	Network Anomalies and Attacks	**6.41%**
New link group	Suspicious or Unexpected Network Behavior	**5.73%**
Cleartext password	Authentication and Password Issue	**5.59%**
Multiple access denied events	Access Control and Authorization	**5.06%**
New link	Suspicious or Unexpected Network Behavior	**3.83%**
New OT variable value	OT Specific Threats	**3.11%**
New target node	Suspicious or Unexpected Network Behavior	**3.08%**

3.2 Industry Insights

In this section, we enumerate the threats targeting specific industries. Only industries where Nozomi Networks has a statistically significant customer base providing telemetry data are included.

Here are the top five industries where our customers experienced the highest number of alerts per customer for the specified period:

1. Industrial Machinery & Equipment
2. Building Materials
3. Chemicals & Related Products
4. Custom Software & IT Services
5. Electricity, Oil & Gas

As in the previous reporting period, the Industrial Machinery & Equipment sector experienced the highest number of alerts among the five industries we analyzed. The Retail and Food & Beverage sectors were replaced in the top five chart by Building Materials and Chemicals. Electricity, Oil & Gas remained in fifth place.

Regardless of relative ranking, each industry faces threats and attacks tailored to that environment. It is extremely important to know your environment and deploy solutions and policies that protect against them.

Industrial Machinery & Equipment

Alert type	Alert category	Percentage
Illegal parameters request	OT Specific Threats	**47.13%**
Malformed traffic	Network Anomalies and Attacks	**32.56%**
TCP flood	Network Anomalies and Attacks	**8.50%**
Network scan	Network Anomalies and Attacks	**3.21%**
Multiple access denied events	Access Control and Authorization	**2.89%**

Building Materials

Alert type	Alert category	Percentage
Cleartext password	Authentication and Password Issue	**31.56%**
Network scan	Network Anomalies and Attacks	**24.18%**
Multiple access denied events	Access Control and Authorization	**19.15%**
TCP flood	Network Anomalies and Attacks	**17.55%**
Missing variable request	OT Specific Threats	**1.93%**

Chemicals & Related Products

Alert type	Alert category	Percentage
Missing variable request	OT Specific Threats	**31.63%**
Network scan	Network Anomalies and Attacks	**22.65%**
Cleartext password	Authentication and Password Issue	**15.78%**
New target node	Suspicious or Unexpected Network Behavior	**4.49%**
New function code	OT Specific Threats	**3.47%**

Electricity, Oil & Gas

Alert type	Alert category	Percentage
Missing variable request	OT Specific Threats	**54.46%**
Variable flow anomaly	OT Specific Threats	**10.10%**
TCP flood	Network Anomalies and Attacks	**9.40%**
Network scan	Network Anomalies and Attacks	**3.22%**
New link group	Suspicious or Unexpected Network Behavior	**3.07%**

Custom Software & IT Services

Alert type	Alert category	Percentage
Link RST request by producer	Network Anomalies and Attacks	**17.40%**
Producer sync request by consumer	Network Anomalies and Attacks	**15.58%**
Weak password	Authentication and Password Issue	**13.02%**
New target node	Suspicious or Unexpected Network Behavior	**11.48%**
New node	Suspicious or Unexpected Network Behavior	**7.15%**

3.3 Regional Insights

This section explores regional variances in security issues by looking at the top five countries with the highest number of alerts per customer. Again, we only evaluated countries where we have a significant number of customers sharing anonymized telemetry data. Out of them, the top countries with the highest average number of alerts per customer are Italy, Spain, Colombia, Sweden and the United States.

Following are the top five alerts raised and associated threats detected per customer in each of these countries. As we saw in our industry-level analysis, each country has its own profile of top threats.

For example, in Italy the top three alert types raised were OT-specific, whereas in the U.S. the top issues raised were associated with Network Anomalies and Attacks.

To make informed decisions when prioritizing issues, pay attention to the situation specific to both your region and industry.

Italy

Alert type	Alert category	Percentage
Missing variable request	OT Specific Threats	**95.15%**
Unsupported function request	OT Specific Threats	**2.79%**
Illegal parameters request	OT Specific Threats	**0.75%**
Malformed traffic	Network Anomalies and Attacks	**0.50%**
TCP flood	Network Anomalies and Attacks	**0.32%**

Spain

Alert type	Alert category	Percentage
Missing variable request	OT Specific Threats	**84.66%**
Malformed traffic	Network Anomalies and Attacks	**6.73%**
Network scan	Network Anomalies and Attacks	**2.19%**
Cleartext password	Authentication and Password Issue	**1.73%**
TCP flood	Network Anomalies and Attacks	**1.18%**

Colombia

Alert type	Alert category	Percentage
Illegal parameters request	OT Specific Threats	**99.46%**
New link group	Suspicious or Unexpected Network Behavior	**0.10%**
New link	Suspicious or Unexpected Network Behavior	**0.09%**
New target node	Suspicious or Unexpected Network Behavior	**0.08%**
New OT variable value	OT Specific Threats	**0.04%**

United States

Alert type	Alert category	Percentage
Malformed traffic	Network Anomalies and Attacks	**32.29%**
Illegal parameters request	OT Specific Threats	**31.06%**
TCP flood	Network Anomalies and Attacks	**8.51%**
Multiple access denied events	Access Control and Authorization	**5.94%**
Missing variable request	OT Specific Threats	**4.02%**

Sweden

Alert type	Alert category	Percentage
New link group	Suspicious or Unexpected Network Behavior	**34.30%**
New confirmed link	Suspicious or Unexpected Network Behavior	**24.70%**
New link	Suspicious or Unexpected Network Behavior	**23.30%**
TCP flood	Network Anomalies and Attacks	**6.15%**
New OT variable	OT Specific Threats	**4.06%**

4 The IoT Botnet Landscape

In this section we explore IoT threats, drawing insights from a wealth of data gathered between January 1 and May 30, 2024. Nozomi Networks Labs has a strategically deployed, globally distributed chain of honeypots designed to attract and observe malicious activities in the IoT space.

These honeypots are deployed as separate sensors and are not related 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.

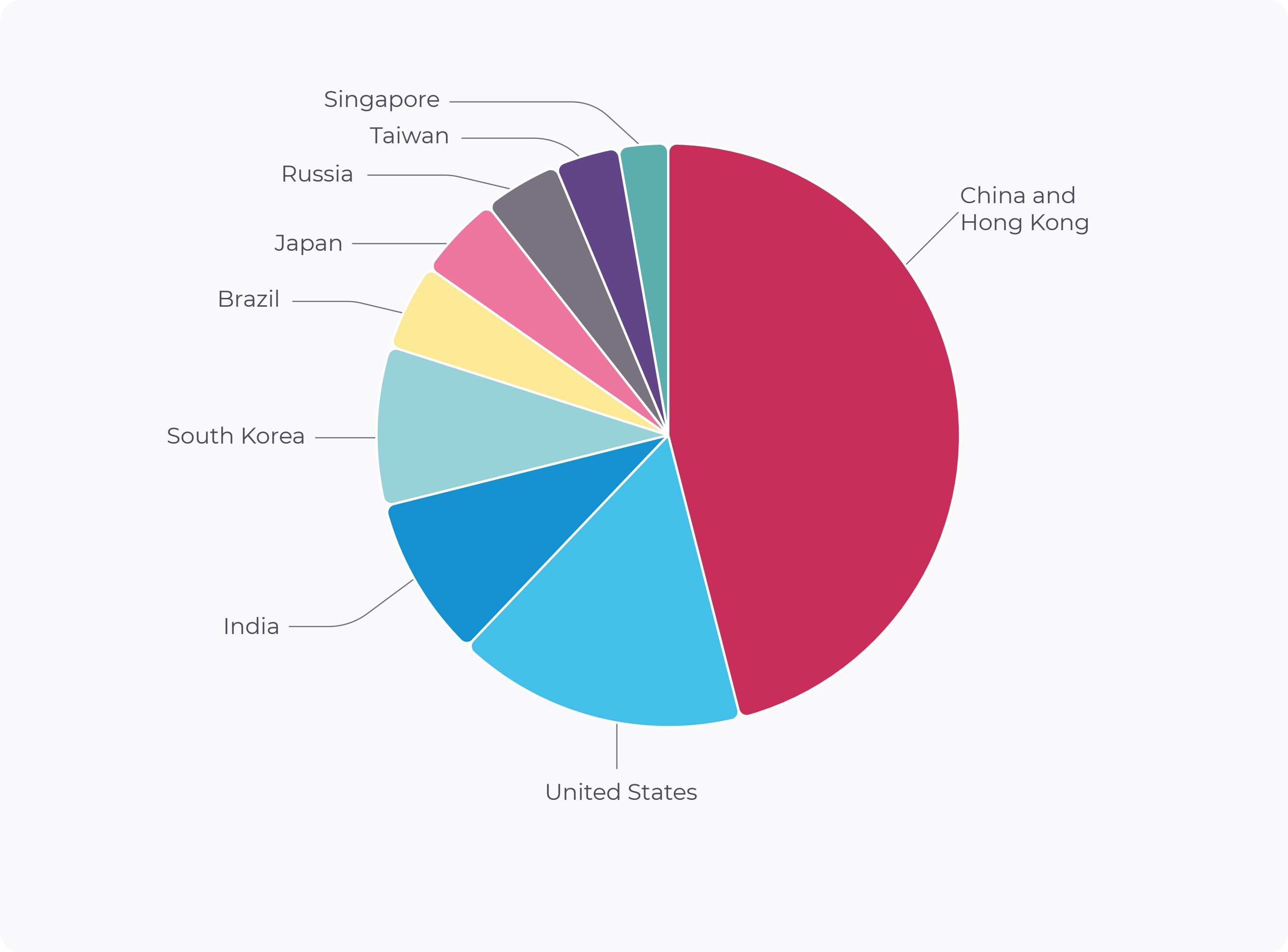
If you’re a Nozomi Networks customer, you are covered for these IoT botnet threats because intelligence regarding them is baked into our product by the Labs team.

4.1 Attack Source Locations

Here, we map the IP addresses from which the attacks against our honeypots were initiated to the countries of origin. Note that the countries with the largest shares of the pie chart do not necessarily have weak cybersecurity postures. On the contrary, countries with high levels of automation typically have more smart devices connected to the internet that may be compromised and become part of a botnet.

The distribution among attack-source countries has changed little since the previous reporting period. China and Hong Kong still dominates at #1 (46%), with the U.S. at #2 (16%). India and South Korea swapped places but are still even at 9%. Notably, Japan jumped from #9 to #5, but only attracted 5% of attacks in our sample.

Remember that in most cases, it is difficult to attribute the associated infrastructure locations with the location of the threat actors. Adversaries and criminal gangs own or rent the actual hardware, and compromise machines in dispersed locations to accumulate more devices under their control and cover their own tracks.

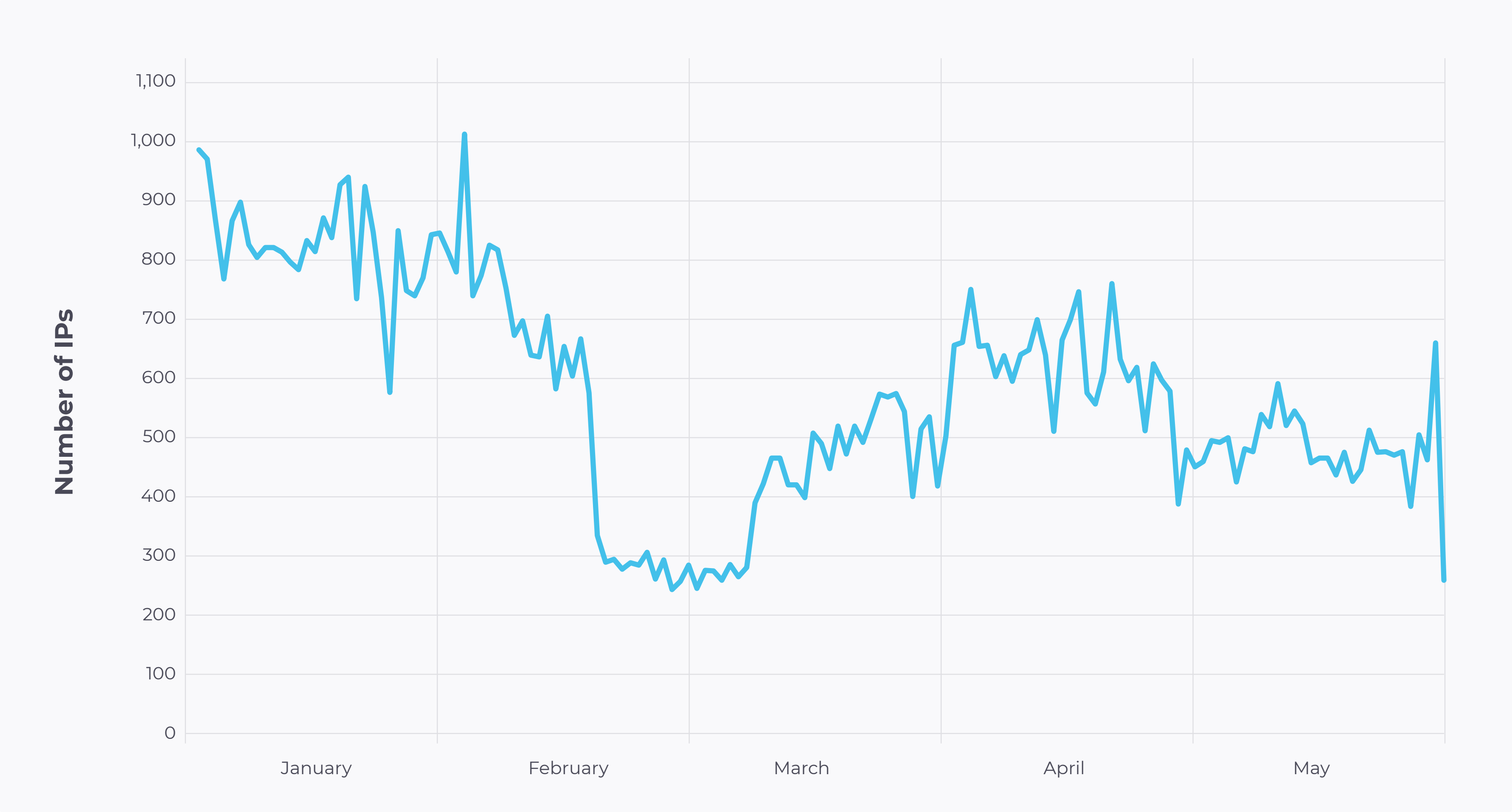


Top countries from where the attacks against honeypots originated (by unique IP addresses).

4.2 Number of Unique Daily Attacker IPs

Looking at the daily activity of IoT botnets over this period, spikes in the chart may represent the appearance of a new botnet or a big improvement in the effectiveness of an existing one.

Over the current period, the average daily number of unique IP addresses initiating attacks on our honeypots was 573, a significant drop compared to the previous period (813). We continue to monitor the situation and aim to promptly ensure protection against all emerging threats before they can cause significant damage to our customers' environments.

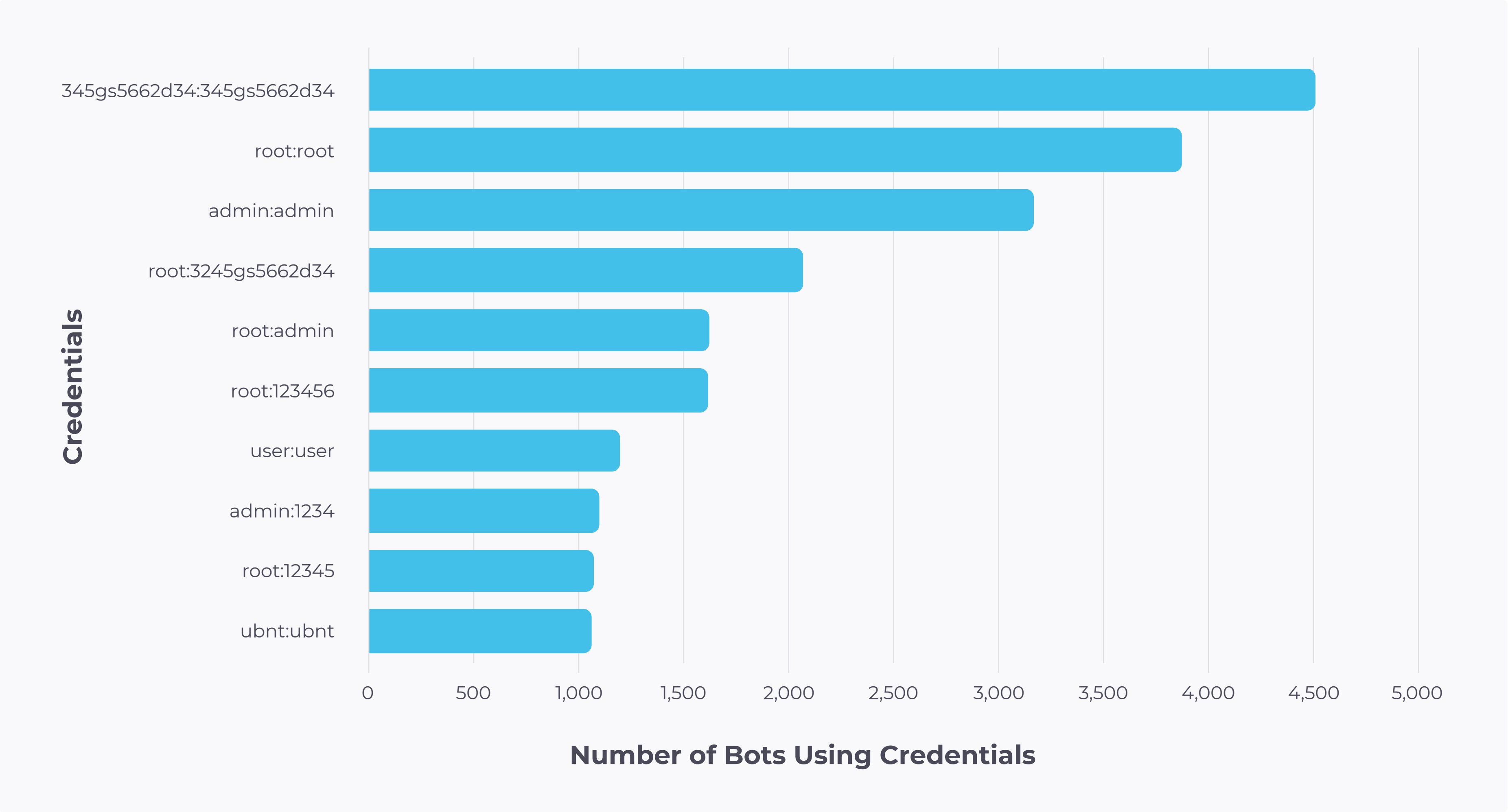


Daily volume and activity from unique attacker IP addresses observed January 1 - May 30, 2024.

4.3 Top Credentials Used

Once botnets establish connectivity, they may try to exploit vulnerabilities to achieve remote code execution or try to brute-force passwords. The chart on the right shows the top pairs of credentials (usernames and passwords) intercepted by our honeypots. Note once again the strange numerical combination of identical username and password 345gS5662d34 that has been a top credential noted in several IoT security reports, including ours. There is some speculation that it's a numerical translation of a default admin username and password, or a honeypot radioactive dye tactic, but the explanation currently remains a mystery.

This is a stark reminder that cybercriminals continue to exploit factory-default or weak passwords to gain access to IoT devices. It's impossible to overstate the importance of following strong credential management practices, beginning with promptly identifying and changing default credentials in all IoT devices (and, of course, IT and OT devices). That includes changing default embedded credentials, especially if they are highlighted in this list.

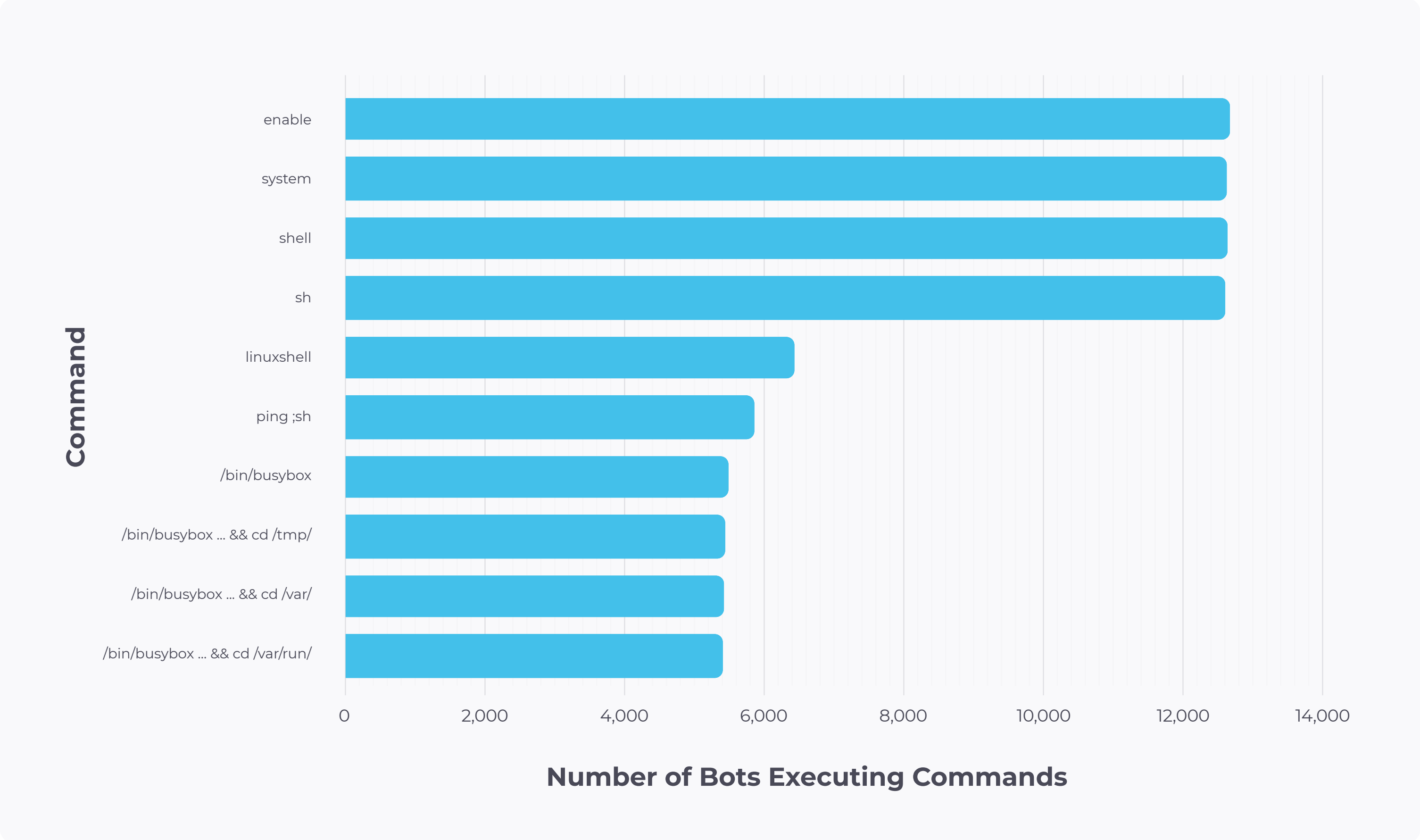


Top credentials used by attackers to get access to honeypots.

4.4 Top Executed Commands

Once attackers have compromised a vulnerable device and obtained initial access, they often start executing shell commands to either explore the environment or achieve persistence and survive reboot or remediation procedures. As usual, the first four commands are seen more than twice as often as the remaining six. `“Enable”`, `“sh”`, `“shell”` and `“system”` are generic auxiliary commands typically executed by attackers to ensure they have the right shell to execute future commands.

The last four commands use BusyBox, an open-source, minimalistic shell that combines tiny versions of nearly 400 common commands into a small executable. Because of its size (less than one MB), it’s popular for embedded devices, including IoT. BusyBox is commonly executed by the Mirai botnet malware (and its clones) to efficiently control and manipulate a system, regardless of the underlying operating system’s specific utilities. Specifically, it executes sequential echo commands to identify the highest-privilege location with available “write” access and store its malicious payload. In the next section we’ll look at what these malicious payloads are.



Top 10 commands executed by attackers once they believe they have established access to honeypots.

** Non-truncated commands:*

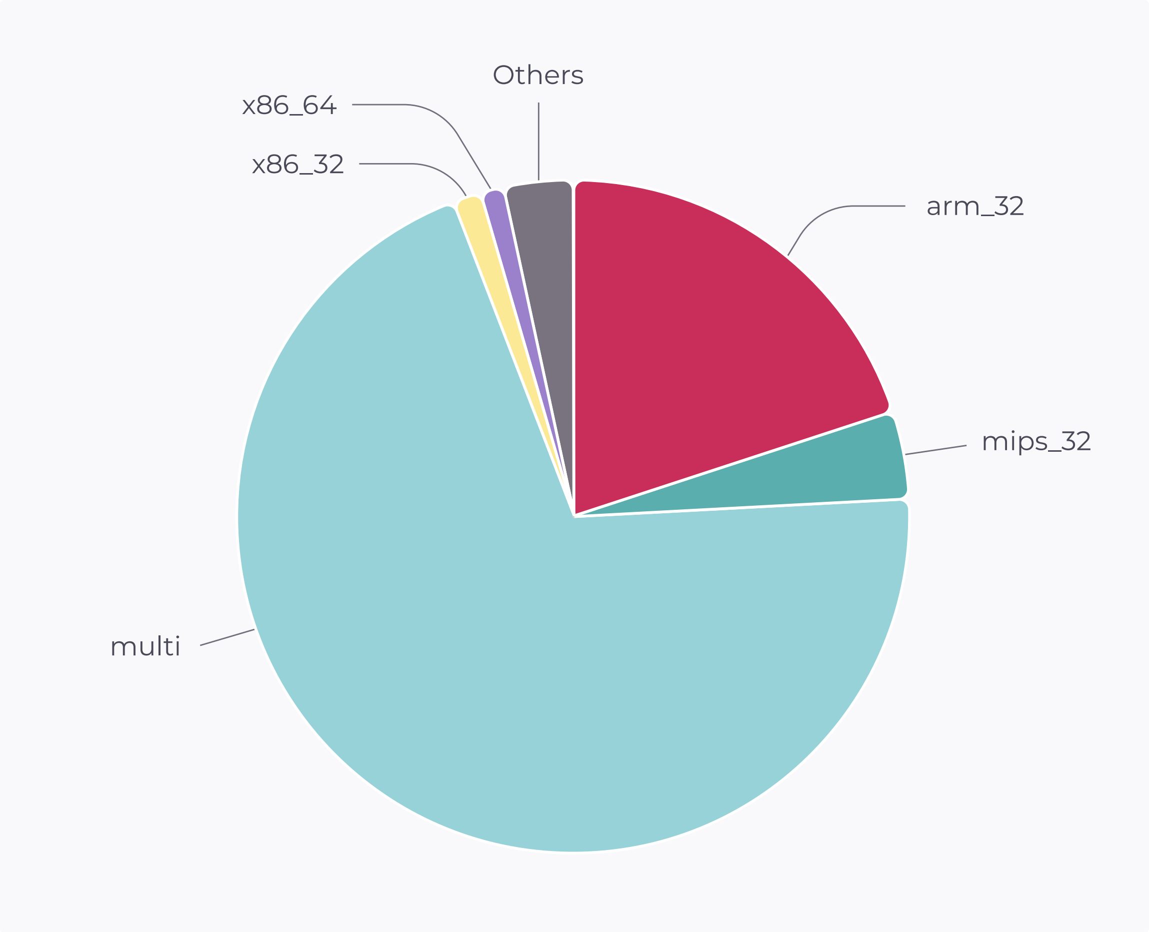
8. /bin/busybox echo > /tmp/.b && sh /tmp/.b && cd /tmp/
9. /bin/busybox echo > /var/.b && sh /var/.b && cd /var/
10. /bin/busybox echo > /var/run/.b && sh /var/run/.b && cd /var/run/

4.5 Top Payload File Types

In this section we look at the distribution of malicious payloads delivered by bad actors to our honeypots once they believe they have successfully compromised them.

The vast majority of payloads are not tied to any one architecture (multi) and generally represent shell scripts that will work equally well on many of them. During this period, multi-architecture payloads overtook 32-bit ARM payloads, which is still the dominant single architecture targeted by attackers.

This is no surprise given ARM's popularity among IoT device manufacturers. Holding steady in third place, with a constant but much smaller share of targeted payloads over the last three reporting periods, is 32-bit MIPS.



Top architectures for which the malicious payloads were created.

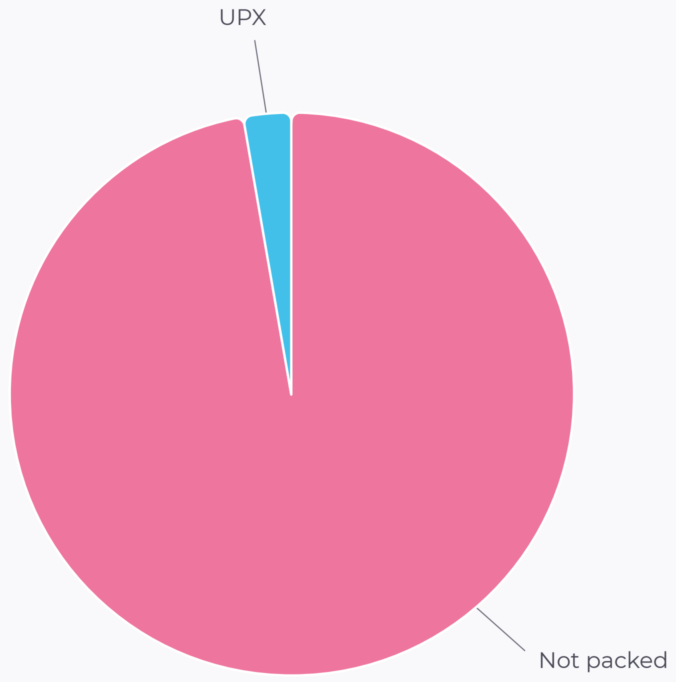
4.6 Top Payload Packers

Packing is a common compression technique used by threat actors to protect their malware from being analyzed and detected. For Windows there are many vendors and products available for this purpose, along with malicious packers created by cybercriminals for cybercriminals to protect malware. In the IoT world, however, the open-source UPX packer continues to be the only free, viable solution available to attackers and, once again, a small slice of malware in our sample was packed by it.

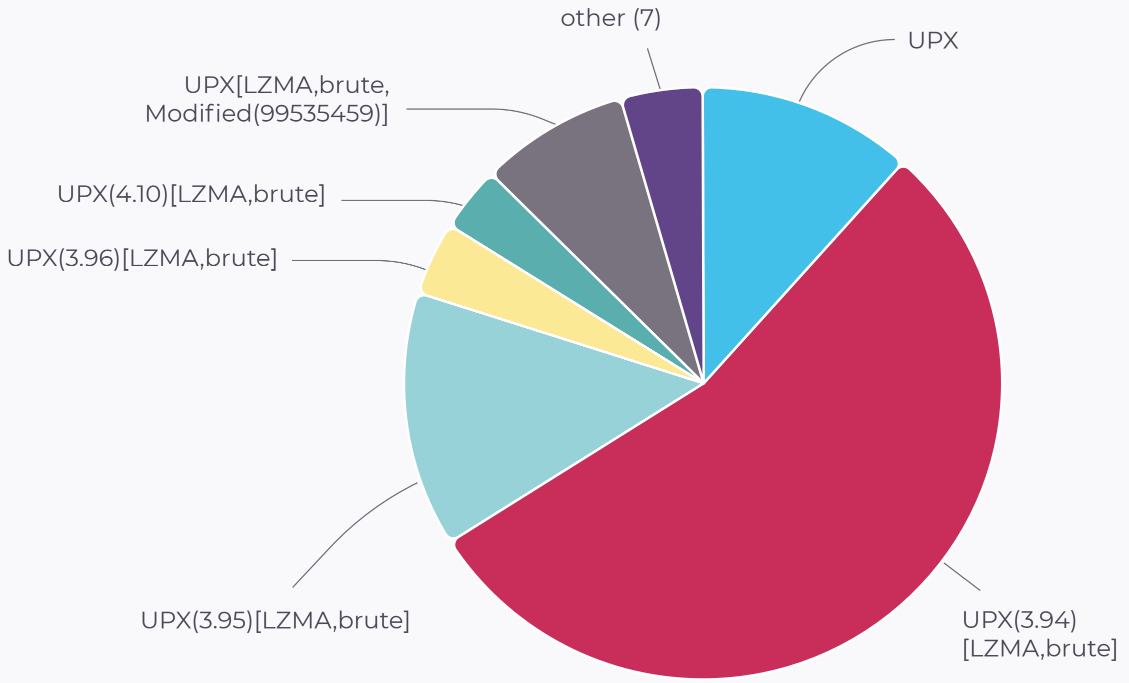
Why don't more threat actors bother to apply it? Probably because it's part of a tool that allows both packing and unpacking of executables, an approach that likely provides little protection.

Even when attackers in our sample did use it, in approximately half of cases they stuck to UPX 3.94, which was released several years ago, rather than the latest version. Still, be sure to always use the latest UPX version in your automation systems to unpack malware to minimize the volume of non-unpacked samples.

Finally, for cases when UPX structures are modified in the packed samples to prevent the standard UPX tool from unpacking them, try the fixing tool that we developed for this purpose: https://github.com/NozomiNetworks/upx-recovery-tool



Top packers used by attackers to protect their malware.



Breakout of UPX packer versions used by attackers to protect their malware.

5. Recommendations

In summary, our findings confirm that organizations can enhance their cybersecurity posture by adopting a holistic cybersecurity strategy that accounts for key differences and considerations unique to OT and IoT networks and devices. This includes automated asset inventory, continuous monitoring, sharing of threat intelligence, incident response plan development and ongoing improvement based on real-world telemetry.

Here are specific actions defenders can take together to remove OT/IoT blind spots, maximize limited resources, increase operational efficiency and resilience, and reduce business risk.

1. Unify your defenses

Embrace a holistic cybersecurity strategy that integrates frameworks relevant to IT, OT and IoT while acknowledging key differences that could cause harm or disruption. Allow these frameworks to guide decisions on the best ways to move forward and prioritize actions.

2. Enhance monitoring, threat detection and response capabilities

Continuously monitor your critical assets, not only in traditional wired networks but also in unplanned ways attackers may try to circumvent security such as wireless, USB and other media. Have playbooks in place to guide response efforts and ensure reliable partners are aligned and already onboard with your mission.

3. Strengthen supply chain and critical infrastructure resilience

Understand that the shifting threat landscape also has implications for surrounding environments, even if detached, and could impact your operations. Be prepared for disruptions in transportation, power, water, on-site labor, communications or other resources, and work to proactively reduce these risks.

4. Reduce consequences

In addition to playbooks and incident response plans, tabletop exercises can help reduce the impact of a breach. Together these measures enable you to streamline processes, identify gaps and ensure the right teams are in place with the right tools, ready to act in a potential crisis.

5. Share threat intelligence

Ensure all defense systems are loaded with the latest threat intelligence feeds to promote team and community collaboration, strength in numbers and a unified front against adversaries. Consider ways to share intelligence from your organization with others, such as through **ETHOS** or an industry-specific **ISAC**.

6. Adopt a post-breach mentality

Recognize that breaches are inevitable. While prevention is crucial, it shouldn't be the only focus of cybersecurity efforts. By planning for the worst-case scenario, organizations can ensure they maintain operations and safety even in the face of successful attacks. This approach also includes continuous improvement of security measures based on lessons learned from past breaches to enhance overall cyber resilience.

7. Repeat employee training and awareness

It's common knowledge that employees are still the weakest link in cybersecurity. Conduct regular training sessions for employees to help them recognize and report suspicious activities. Promote a security-aware culture within the organization to reduce the risk of insider threats and social engineering attacks.

8. Keep your adversaries in perspective

Nation-state actors often have virtually unlimited resources, skills and tools to conduct operations. They actively work by hand, living off the land and passing as mundane, normal activities. What does that say about some of the seemingly minor indications and anomalies identified in this report? Don't discard them. They may be red flags or other clues that an APT is present, biding time.

Nozomi Networks is here to help

From day one, Nozomi Networks' solutions have been deeply rooted in addressing the complex requirements of industrial and critical infrastructure environments.

As OT converges with the vastly different worlds of IT and IoT, that experience has given us a unique understanding of the tools and processes associated with the largest networks in the world. We've earned a global reputation for unmatched service, superior cyber and physical system visibility, advanced OT and IoT threat detection, and scalability across distributed environments.

We provide **real-time asset visibility**, **threat detection** and **actionable intelligence** that keeps you in control of your critical infrastructure.

Learn more →

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