NOZOMI NETWORKS LABS

OT & IoT SECURITY REPORT

Assessing the Threat Landscape

February 2024 | Second Half 2023 Review

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

The stakes are rising for industrial and critical infrastructure security. As threat actors increase their attack frequency, they're also refining their tactics and finding new access points. While ransomware attacks remain high, it's now commonplace to see attacks motivated by control and destruction.

According to Microsoft, last year 120 countries faced cyberattacks fueled by nation-state actors – more than 40% were leveled against critical infrastructure. And, as we prepared to publish this report, FBI Director Christopher Wray warned Congress that Chinese hackers are "preparing to cause real-world harm to American critical infrastructure." It's a global risk that we've been watching and according to Wray, "It's a risk that requires attention now."

This report summarizes findings based on ICS vulnerabilities released by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), as well as telemetry data from Nozomi Networks-deployed monitoring and detection software in enterprise and operational technology (OT) networks. It also describes additional findings from Nozomi Networks Labs distributed honeypot deployments, tracking and analyzing the latest patterns in IoT technology hijacking, abuse and misuse.

In the second half of 2023, **network anomalies and attacks** were the most prevalent threat to OT and IoT environments. Vulnerabilities within **critical manufacturing** also surged 230% – a cause for concern as threat actors have far more opportunities to access networks and cause these anomalies. Nozomi Networks Labs also analyzed a wealth of data on malicious activities against IoT devices and botnets continue to use default credentials in attempts to access IoT devices. **Brute-force** attempts remain a popular technique to gain system access – **default credentials** remain one of the main ways threat actors gain access to IoT. **Remote Code Execution (RCE)** also remains a popular technique – it's frequently used in targeted attacks, as well as in the propagation of various types of malicious software.

Adversaries targeting industrial control systems continue to deploy **living-off-the-land attacks** that are "cheaper to deploy, have higher success rates, are more difficult to detect, require more rapid industrial response, and can have immediate direct safety and engineering impacts."

In order to live off the land, you have to get to know the landscape. In order to defend the landscape, you have to know it better than your adversary. The findings in this report are designed to help you do just that.

2

The Vulnerability Landscape

As our world becomes more and more interconnected, various industries are embracing automation and introducing devices, both wired and wireless, to enhance processes and streamline workflows. Unfortunately, too many of these devices are insecure and provide opportunities for attackers to disrupt normal operations with potentially devastating consequences.

Across the globe, security researchers including the team at Nozomi Networks Labs work every day to outpace attackers. The goal is to find and report these vulnerabilities so they can be addressed before threat actors discover and misuse them. Reviewing the industry's continuous work toward this goal, this section provides a detailed analysis of all the ICS security advisories released by CISA over the past six months.

For this period (July 1, 2023 – December 21, 2023), CISA released **196** new ICS advisories mentioning **885** old and new vulnerabilities affecting products from **74** vendors. Taking a closer look at them, we found reported CVEs were up 38% compared to the first half of 2023, while mentioned vendors went up 19% from the first half of 2023.

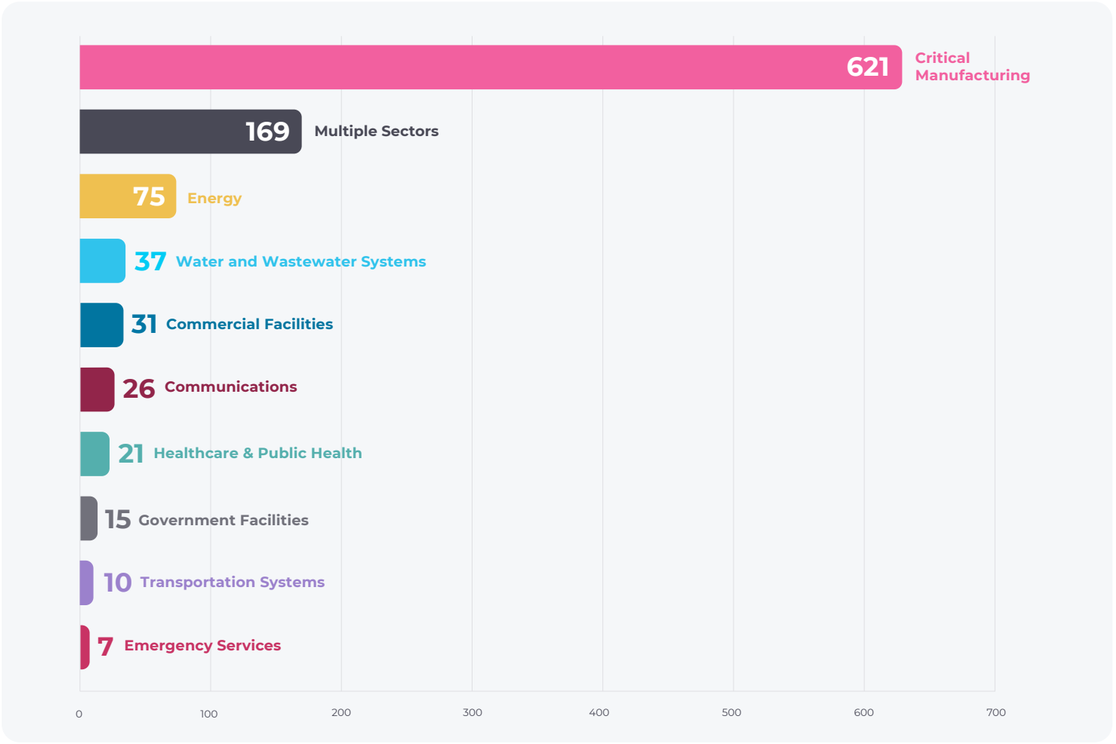
2.1 Number of CVEs Released by Sector

Critical Manufacturing topped the list of most vulnerable industries with the number of reported Common Vulnerabilities and Exposures (CVEs) rising to 621. That's an alarming 230% increase over the previous reporting period. This massive rise in reported vulnerabilities illustrates the considerable challenge this sector faces as it continues to embrace digitalization. There's an urgent need for critical manufacturers to invest in robust cybersecurity measures capable of covering potential attacks from the endpoint to the air.

For a third consecutive reporting period, Manufacturing and Energy and Water/Wastewater remained the most vulnerable industries – though the total number of vulnerabilities reported in the Energy sector dropped 46% from the previous period and Water/Wastewater vulnerabilities dropped 16%. Of note, Healthcare & Public Health, Government Facilities, Transportation Systems and Emergency Services all made the top 10.

It's worth mentioning that some vulnerabilities affect several of these sectors and therefore contribute to the total number of each of them. The Multiple Sectors category (with 169 vulnerabilities) encompasses a diverse range of industries and is a reminder that in many cases, a significant number of CVEs impact multiple sectors.

These latest figures underscore the intricate web of cybersecurity challenges faced by different industries and remind us of the need for concerted efforts to fortify defenses and mitigate potential risks across the board. As cybersecurity experts, it is imperative that we recognize and address these vulnerabilities with strategic and targeted initiatives to ensure the resilience of our critical systems.



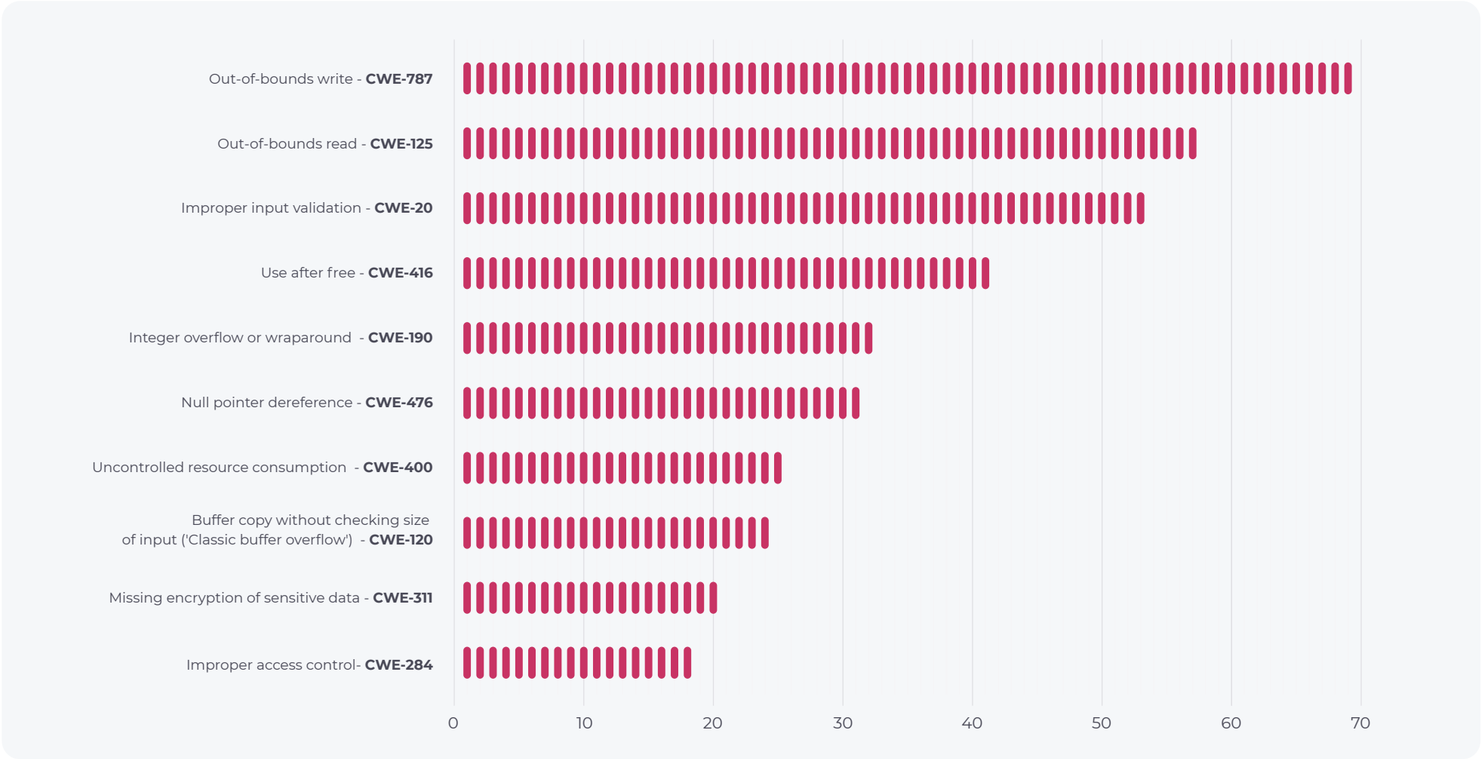
Top 10 industries with most reported vulnerabilities in the second half of 2023.

2.2 Number of CWEs Associated with CVEs

The Common Weakness Enumeration (CWE) classification categorizes types of vulnerabilities. This allows developers to focus on the core reasons behind them and address those issues to create more secure products.

In our previous report, the most common CWE category was USE AFTER FREE. This was surprising as it's not the easiest vulnerability for researchers to discover. This time, USE AFTER FREE dropped to fourth place with OUT-OF-BOUNDS WRITE and READ leading the chart. Both weaknesses are children of IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER (CWE-119). They are closely related, among others, to BUFFER OVERFLOW, a well-known and commonly introduced vulnerability.

Finally, IMPROPER INPUT VALIDATION (CWE-20) came in third. This is a high-level weakness type and has many "children" CWE IDs, commonly followed by other weaknesses like IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS, an example of which would be SQL injections. As we saw in our previous report, these three CWEs remain the most common weaknesses affecting various categories of products.



Top 10 IDs associated with vulnerabilities reported from July - December 2023.

3 Attack Statistics from OT Environments

In this section, we delve into the current landscape of OT cybersecurity monitoring, leveraging anonymized Nozomi Networks telemetry submitted by participating customers.

These statistics shed light on emerging OT security trends, the threat landscape, and the resilience of industrial systems. Below we detail the nuances of attacks in ICS environments, empowering organizations with information that can be used to better fortify defenses.

3.1 Commonly Detected Malware

Here we take a look at the list of malware that remains prevalent in all domains over the last six months. We cover four domains: ENTERPRISE (aka IT), OT (aka ICS) IoT and a MULTI domain category, which represents malware threats that cannot be attributed to a specific domain.

In the ENTERPRISE domain, malicious worms remain a very common threat, responsible for about half of all malware-related alerts raised by Nozomi Networks products. The distinctive feature of worms is their ability to automatically propagate across multiple machines, where the same or very slightly modified sample is being distributed over networks. In second place, the TROJAN category is an umbrella term representing different types of malware. Finally, DUALUSE takes the third place in our chart, represents tools commonly used by attackers, but which may also be used by administrators for legitimate network maintenance (like PsExec tool by SysInternals).

Top Malware Categories - Enterprise

Malware	Number of Detections
Worm	**48.87%**
Trojan	**40.65%**
Dualuse	**10.34%**
Ransomware	**0.08%**
RAT	**0.03%**
Exploit	**0.02%**
Webshell	**0.01%**
Hacktool	**0.01%**

Looking at top OT malware, the universal TROJAN category leads the chart, while Denial of Service (DoS) threats take the second place. It is quite common to find this type of malware involved in ICS attacks where attackers try to disrupt the processes by causing hardware or software to stop operating.

In the IoT domain, Distributed Denial of Service (DDoS) attacks were the only attacks we saw. This is the most common way attackers

Top Malware Categories - OT

Malware	Number of Detections
Trojan	**80%**
DoS	**20%**

may monetize compromised IoT devices, by launching paid attacks against websites and other targets trying to make them inaccessible due to the high number of requests sent from various places across the globe.

Top Malware Categories - IoT

Malware	Number of Detections
DDoS	**100%**

Finally, our MULTI domain category has cryptocurrency miners (MINER) as a top threat that commonly affects multiple sectors. That's because attackers may not necessarily care where the compromised device is located and its original function, as long as its computational power can be misused to gain profits. MINER is followed by WEBSHELLs, which can be deployed in multiple domains, as well as more generic SUSPICIOUS activity representing various less definitive patterns.

Top Malware Categories - Multi

Malware	Number of Detections
Miner	**22.99%**
Webshell	**21.84%**
Suspicious	**20.69%**
Phishing	**17.24%**
Scanner	**9.20%**
RAT	**6.90%**
Dualuse	**1.15%**

3.2 Types of Intrusion Alerts

In order to understand what problems were most reported in OT and IoT environments, this section takes a look at the top alerts raised by Nozomi Networks products across all our participating customers. We exclude malware-related attacks as we covered them in the previous section.

Let us start with the top 10 types of issues reported, which account for almost 80% of all alerts during this period. In this report, we exclude alert types representing Nozomi Networks technologies like “Packet rule match” in order to focus on alerts related to security issues. In addition, instead of using absolute numbers, we look at the percentage of each alert in comparison to total alerts over the past six months.

When you consider the 10 most common alert types we saw in customer environments, Network scanning activity tops the chart, associated with around one fifth of all alerts.

This is similar to what we found in the first half of 2023, where this alert type also topped the list. Network scanning can be performed by both malevolent attackers and dedicated red teams, so it may or may not represent a legitimate threat, depending on the organization.

Overall, alert types in the 'Network Anomalies and Attacks' category comprise the most significant proportion of the total number of alerts raised. Setting aside "Network scan" alerts which saw a significant decline over the previous reporting period, all other alerts in this category increased 19% over the previous reporting period.

Top 10 Most Critical Types of Intrusion Alerts

July to December 2023

Alert type	Alert category	Percentage
Network scan	Network Anomalies and Attacks	**19.55%**
Cleartext password	Authentication and Password Issue	**14.63%**
TCP flood	Network Anomalies and Attacks	**10.20%**
Multiple access denied events	Access Control and Authorization	**9.61%**
Malformed traffic	Network Anomalies and Attacks	**8.42%**
Weak password	Authentication and Password Issue	**4.60%**
Device state change	Operational Technology (OT) Specific Threats	**4.24%**
New link group	Suspicious or Unexpected Network Behavior	**3.22%**
Program transfer	Operational Technology (OT) Specific Threats	**2.80%**
New target node	Suspicious or Unexpected Network Behavior	**2.52%**

Network Anomalies and Attacks

While "Network scan" topped the list for a second consecutive reporting period, TCP flood attacks, another alert in the 'Network Anomalies and Attacks' category were also high on the list, coming in third. These types of attacks involve sending large amounts of traffic to systems aiming to cause damage by bringing down important systems and making them inaccessible. "TCP flood" and "Anomalous packets" alert types exhibit significant increases in both total alerts and averages per customer in the latest period. "TCP flood" alerts increased by more than 2x over the latest report and anomalous packet alerts saw a 6x increase.

While "TCP flood" attacks are common in ICS systems, the alert trends we saw in the last six months indicate evolving network threats, possibly reflecting adaptive attacker strategies or heightened detection capabilities.

As customers resolve low hanging fruit issues, like passwords in clear text, they pursue more advanced monitoring capabilities such as anomaly detection and protocol inspection. Increases in this alert category reflect a maturity in the monitoring capabilities of our customers.

Authentication and Password Issues

Poor credential management like cleartext passwords being transferred over non-encrypted channels as well as weak passwords being used is another common problem historically plaguing OT devices designed without sufficient cybersecurity considerations. While "Cleartext password" alerts remain high on the list of common alert types, for a second consecutive reporting period we saw a significant decrease in the average number of these alerts per customer, with a 33% reduction from the previous report. This suggests improved security measures or changing attack patterns. As soon as Nozomi Guardian sensors start seeing the network, alerts expose these insecure password behaviors, making it easy to improve them.

Authentication Issues

Finally, it's worth noting that though they didn't make the list of 10 most common alerts, "Multiple unsuccessful logins" and "Brute force attack" alerts showed an increasing trend in alert numbers, up 71% and 14% respectively compared the previous reporting period. This could be indicative of the growing challenges in unauthorized access attempts, showing that Identity and Access Management in OT, or other challenges associated with user passwords is an ongoing effort. Although unsuccessful logins could indicate user mistakes, misconfigured service accounts, or other benign events, the increase in brute force attacks in correlation with the other alerts is a double-edged sword. On one side it indicates that the defenses are working, preventing someone from getting in, but on the other side, there's someone at the door trying to get in.

Finally, less common alerts like "New link group" and "New target node" represent potentially suspicious changes in the OT environment, for example a pair of devices suddenly begin communicating to each other or new devices being added, which are worth confirming as they may represent an ongoing attack taking place.

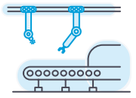
3.3 Industry Insights

When we analyzed the industries with the highest number of alerts per customer, we found Industrial Machinery & Equipment topped the list followed by Retail, Custom Software & IT Services, Food & Beverage and Electricity, Oil & Gas. This section provides a more granular view into specific threats we saw in these top reporting sectors so that you can learn from your peers and pinpoint areas where you may want to focus your cybersecurity defenses.

Alert types are ranked by the total number of alerts per customer. We evaluated industries where we have at least 3 customers participating in anonymized information sharing. In addition, instead of using absolute numbers of alerts, we use the percentages of each alert type per customer relative to the total number of alerts.

In general, our analysis found that many attack types are repeated across sectors, such as malformed traffic or poor credential management, which includes weak passwords or cleartext passwords passed via non-encrypted channels, making them susceptible to sniffing.

At the same time, each industry has its own unique profile of more prevalent threats, which organizations in these sectors may want to prioritize first. The Custom Software & IT *Services* industry stands out, as companies in this sector rarely utilize OT devices but instead commonly use lots of IoT devices plugged in on an ad-hoc basis. This increases the chance of rogue devices being present.



Industrial Machinery & Equipment

Alert type	Alert category	Percentage
Multiple access denied events	Access Control and Authorization	**14.86%**
TCP flood	Network Anomalies and Attacks	**14.49%**
Device state change	Operational Technology (OT) Specific Threats	**12.72%**
Malformed traffic	Network Anomalies and Attacks	**11.21%**
Cleartext password	Authentication and Password Issue	**11.07%**

Top 5 alert types raised in the Industrial Machinery & Equipment industry (avg. per customer).

Retail

Alert type	Alert category	Percentage
Malformed traffic	Network Anomalies and Attacks	**53.51%**
Weak encryption	Access Control and Authorization	**24.28%**
Weak password	Authentication and Password Issue	**9.33%**
Anomalous packets	Network Anomalies and Attacks	**5.02%**
Multiple unsuccessful logins	Access Control and Authorization	**3.88%**

Top 5 alert types raised in the Retail industry (avg. per customer).

Custom Software & IT Services

Alert type	Alert category	Percentage
New link group	Suspicious or Unexpected Network Behavior	**16.62%**
New link	Suspicious or Unexpected Network Behavior	**16.01%**
New node	Suspicious or Unexpected Network Behavior	**13.25%**
New target node	Suspicious or Unexpected Network Behavior	**12.14%**
Link RST request by Producer	Network Anomalies and Attacks	**10.73%**

Top 5 alert types raised in the Custom Software & IT Services industry (avg. per customer).

Food & Beverage

Alert type	Alert category	Percentage
Multiple access denied events	Access Control and Authorization	**21.31%**
Network Scan	Network Anomalies and Attacks	**20.50%**
Missing variable request	Operational Technology (OT) Specific Threats	**15.06%**
Unsupported function request	Operational Technology (OT) Specific Threats	**13.33%**
Cleartext password	Authentication and Password Issue	**6.51%**

Top 5 alert types raised in the Food & Beverage industry (avg. per customer).

Electricity, Oil & Gas

Alert type	Alert category	Percentage
Missing variable request	Operational Technology (OT) Specific Threats	**21.98%**
Network scan	Network Anomalies and Attacks	**18.53%**
Malformed traffic	Network Anomalies and Attacks	**13.67%**
Duplicated IP	Network Anomalies and Attacks	**13.27%**
TCP flood	Network Anomalies and Attacks	**8.06%**

Top 5 alert types raised in the Electricity, Oil & Gas industry (avg. per customer).

3.4 Regional Insights

This section explores how much top security issues deviate from country to country. In this report we feature the top five countries with the highest number of alerts per customer. In the past six months Brazil topped the list with the highest number of threat alerts, followed by Germany, Great Britain, the United States and Italy.

Alert types are ranked by the total number of alerts per customer. We evaluated countries where we have at least three customers participating in anonymized information sharing. In addition, instead of using absolute numbers of alerts, we use the percentages of each alert type per customer relative to the total number of alerts.

The following diagrams illustrate the top five countries that raised the highest number of alerts per customer in the past six months and the top five associated threats detected in each of them. Our analysis finds that while some issues like poor credential management are common across many countries, as we saw in our industry-level analysis, each country has its own profile of top threats.

The main takeaway from these findings is that it is extremely important to understand your environment, as each one has unique features compared to others and to ensure your security solutions are versatile enough to support all of them.

Brazil

Alert type	Alert category	Percentage
Cleartext password	Authentication and Password Issue	**47.11%**
TCP flood	Network Anomalies and Attacks	**12.25%**
Program transfer	Operational Technology (OT) Specific Threats	**9.78%**
Missing variable request	Operational Technology (OT) Specific Threats	**4.61%**
Protocol packet injection	Network Anomalies and Attacks	**3.20%**

Top 5 alert types raised in Brazil (avg. per customer).

Germany

Alert type	Alert category	Percentage
Malformed traffic	Network Anomalies and Attacks	**25.18%**
Multiple access denied events	Access Control and Authorization	**19.57%**
Network scan	Network Anomalies and Attacks	**18.04%**
Unsupported function request	Operational Technology (OT) Specific Threats	**11.61%**
Missing variable request	Operational Technology (OT) Specific Threats	**9.74%**

Top 5 alert types raised in Germany (avg. per customer).

Great Britain

Alert type	Alert category	Percentage
Malformed traffic	Network Anomalies and Attacks	**34.32%**
Multiple access denied events	Access Control and Authorization	**29.10%**
TCP flood	Network Anomalies and Attacks	**12.46%**
New link group	Suspicious or Unexpected Network Behavior	**4.58%**
New link	Suspicious or Unexpected Network Behavior	**4.53%**

Top 5 alert types raised in the UK (avg. per customer).

United States

Alert type	Alert category	Percentage
Cleartext password	Authentication and Password Issue	**17.79%**
TCP flood	Network Anomalies and Attacks	**15.93%**
Weak password	Authentication and Password Issue	**15.70%**
Multiple access denied events	Access Control and Authorization	**15.29%**
Network scan	Network Anomalies and Attacks	**8.03%**

Top 5 alert types raised in the US (avg. per customer).

Italy

Alert type	Alert category	Percentage
Illegal parameters request	Operational Technology (OT) Specific Threats	**24.87%**
Malformed traffic	Network Anomalies and Attacks	**23.27%**
Program transfer	Operational Technology (OT) Specific Threats	**12.14%**
Weak encryption	Access Control and Authorization	**9.37%**
Multiple unsuccessful logins	Access Control and Authorization	**8.36%**

Top 5 alert types raised in Italy (avg. per customer).

4

The IoT Botnet Landscape

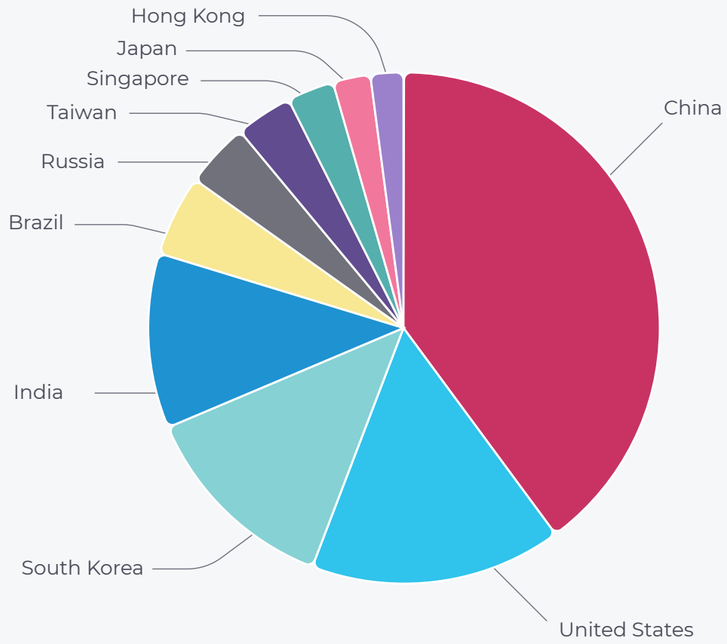
In this section we explore IoT threats, drawing insights from a wealth of data gathered over the past six months (between July 1, 2023 and December 21, 2023). Nozomi Networks Labs has a strategically deployed, globally distributed chain of honeypots designed to attract and observe malicious activities in the IoT space.

These honeypots are deployed as separate sensors and not related to our customers' environments. From this unique 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.

4.1 Attack Source Locations

Here, we mapped all the IP addresses from which the attacks against our honeypots were initiated to the corresponding countries. As usual, it is worth reminding readers that the countries taking a larger proportion of this chart do not necessarily have a worse cybersecurity posture, as we operate with absolute numbers. In countries with more widespread automation, it is natural that the total number of smart devices connected to the internet is higher, resulting in a bigger attack surface, which may result in more devices being compromised.

We can see that highly industrial countries with a high level of automation like China, United States and South Korea continue to lead the chart, the same as in the previous six-month period. Regarding the next three countries, there are some interesting changes compared to the first half of 2023. In particular, Taiwan has moved from fourth place to seventh, indicating that the number of infected machines decreased drastically there, with India, Brazil and Russia moving one step up in the same order as before. Finally, the last two countries have changed completely: Japan and Hong Kong reported a higher number of infected machines, replacing Germany and Vietnam.



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

4.2 Number of Unique Daily Attacker IPs

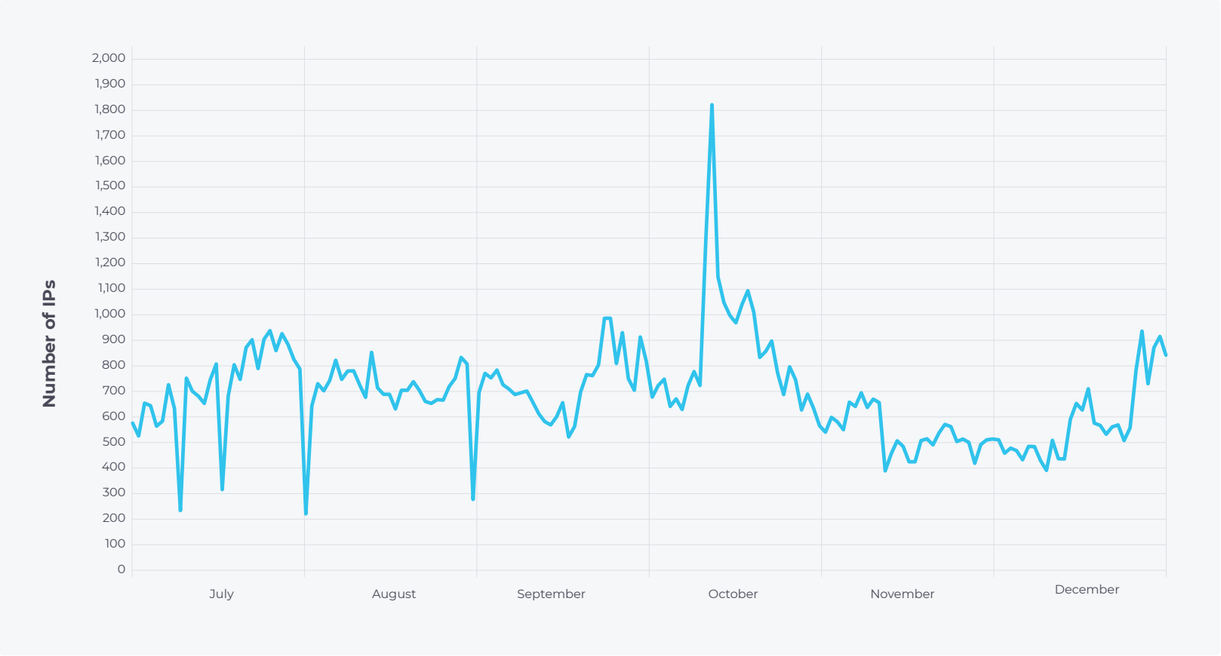
Nozomi Networks constantly monitors the landscape of IoT threats to detect any anomalous spikes that may represent either an ongoing attacks or the appearance of new botnets. In the second half of 2023, malicious IoT botnets remained active. Nozomi Networks Labs uncovered growing security concerns as botnets continue to use default credentials in attempts to access IoT devices.

From July through December 2023, Nozomi Networks honeypots found:

- An average of 712 unique attacks daily (a 12% decline in the daily average we saw in the previous reporting period – 813) – the highest attack day hit 1,860 on October 6.
- Top attacker IP addresses were associated with China, the United States, South Korea, India and Brazil.
- Brute-force attempts remain a popular technique to gain system access – default credentials remain one of the main ways threat actors gain access to IoT. Remote code execution (RCE) also remains a popular technique – frequently used in targeted attacks, as well as in the propagation of various types of malicious software.

As we can see, honeypot activity was quite volatile with the number of infected and cleaned up online machines changing on a daily basis. What is particularly interesting here are various upward and downward spikes as they represent significant and sudden changes in the landscape. For example, the appearance of new botnets, or the updates and takedown of existing ones.

You can read all our research dedicated to various IoT malware families in the blog section of our website.

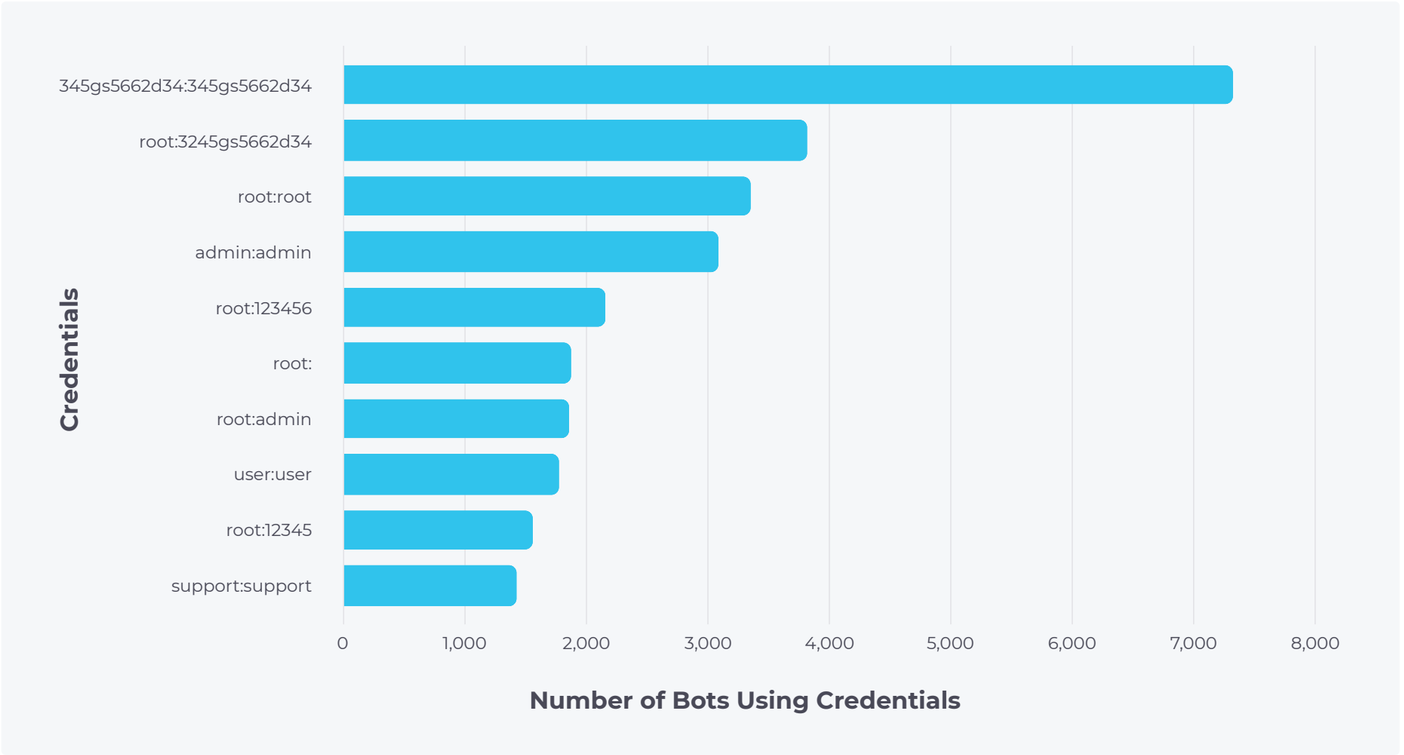


Total number of unique attacker IP addresses Nozomi Networks Labs sensors observed daily between July 2023 and December 2023.

4.3 Top Credentials Used

Once botnets establish connectivity, they may either try to exploit vulnerabilities to achieve remote code execution or try to bruteforce passwords. Below are the top pairs of credentials (usernames and passwords) intercepted by our honeypots that were used by attackers in an attempt to establish control.

This is a stark reminder that cyber criminals are still finding success using factory-default or weak passwords to gain access to IoT devices. It is important for all the organizations regardless of their geolocation and sector to make sure they don't use devices with default embedded credentials present, especially if they are highlighted in this list.



Top credentials used by attackers to get access to honeypots.

4.4 Top Executed Commands

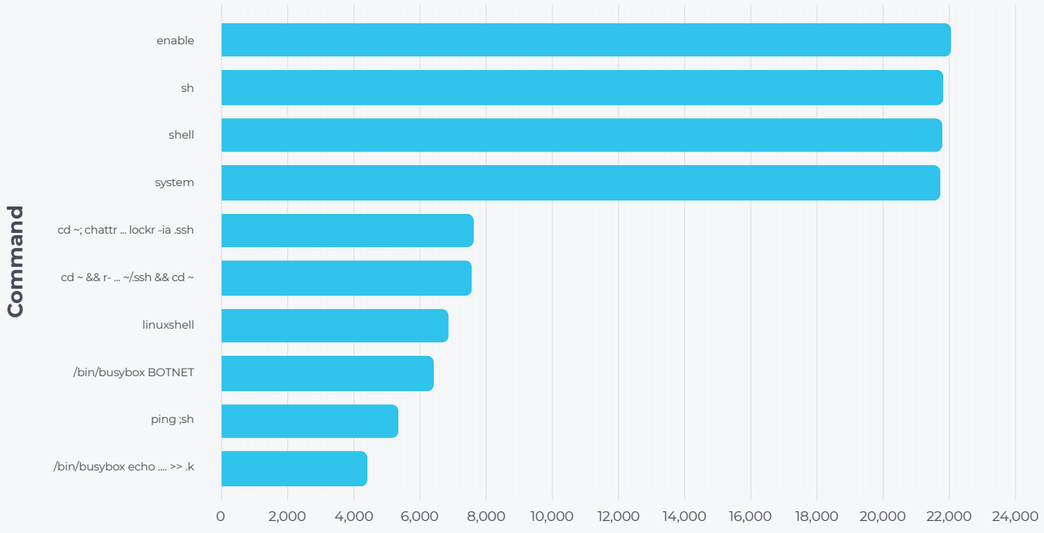
Once attackers believe they have compromised a vulnerable device, they often start executing shell commands to either explore the environment or achieve persistence to survive the reboot or remediation procedures.

While some of them are generic auxiliary commands to enable shell access like the top `"enable"`, `"sh"`, `"shell"` and `"system"`, the others are quite interesting. Here, same as in our previous report, we can see command #6 that adds attackers' public SSH key to the list of authorized keys so that they can connect to the compromised instance later, which can be a valuable indicator of the infection. The last command that involves `"echo"` is one of many similar commands used by malware sequentially to assemble the next stage payload from the specified bytes concatenated to each other.

INSIGHTS

Non-truncated list of commands:

1. enable
2. sh
3. shell
4. system
5. "cd ~; chattr -ia .ssh; lockr -ia .ssh"
6. cd ~ && rm -rf .ssh && mkdir .ssh && echo ""ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUanUV9tJ2/9p7+vD0EpZ3Tz/+0kX34uAx1RV/75GVOmN+9EuWOnvNoaJe0QXxziIg9eLBHpgLMuakb5+BgTFB+rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEmPecjdySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCGPK5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujvcD9iUKQTTWYYjIlu5PmUux5bsZ0R4WFwdle6+i6rBLAsPKgAySVKPRK+oRw== mdrfckr""">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~"
7. linuxshell
8. "/bin/busybox BOTNET"
9. "ping ;sh"
10. "/bin/busybox echo -ne ""\x20\x20\x20\x20\x72\x65\x73\x75\x6C\x74\x3D\x24\x28\x6C\x73\x20\x2D\x6C\x20\x22\x2F\x70\x72\x6F\x63\x2F\x24\x70\x69\x64\x2F\x65"" >> .k"

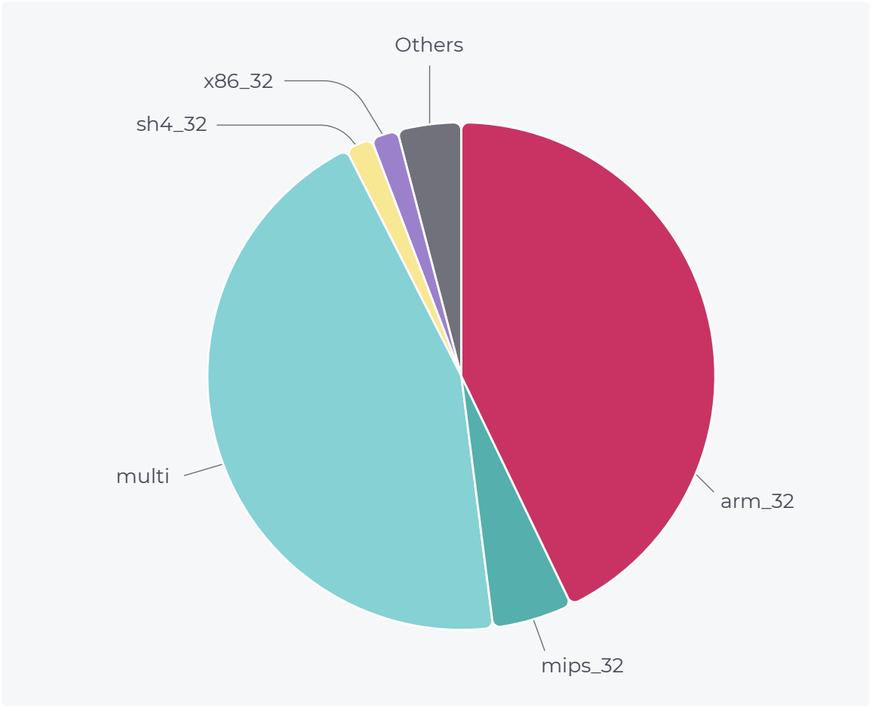


Top 10 commands executed by attackers once they believe they have established access to honeypots.

4.5 Top Payload File Types

Now, let's talk about malicious payloads being delivered by attackers as part of the infection. Here, we can see that attackers preferred utilizing 32-bit ARM ELF payloads.

This matches our findings published in the previous report. 32-bit MIPS payloads take the third place, just as they did six months ago. The multi-architectural payloads (usually shell scripts) are taking a significantly bigger chunk of all the samples collected compared to the previous report.

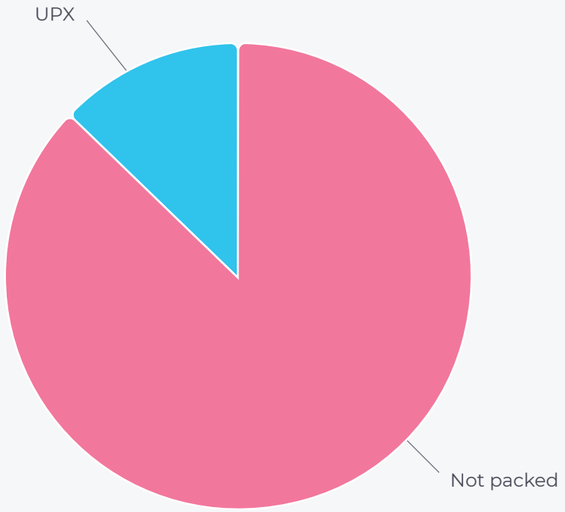


Top architectures for which the malicious payloads were created.

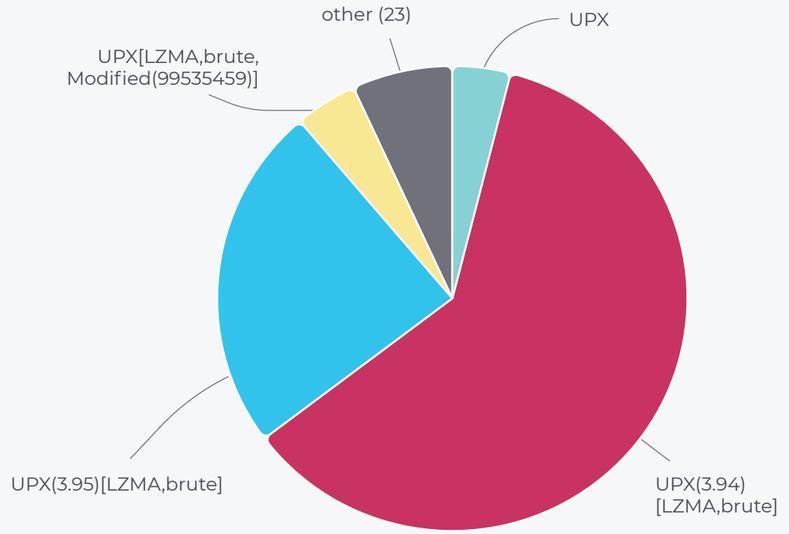
4.6 Top Payload Packers

Finally, let's see how attackers protect their brainchildren from being analyzed and detected. Here, we can see that the open-source UPX packer still remains the leader, being the only viable free solution actively used the attackers.

We can also see that many attackers haven't updated their setups: old UPX versions 3.94 and 3.95 were released several years ago, yet are still the most prevalent. Currently, the latest version of UPX is 4.2.2. Nevertheless, it is important for researchers to use the latest version of UPX in their automated unpackers to be able to cover all the samples collected.



Top packers used by attackers to protect their malware.



Top packers used by attackers to protect their malware (granular).

5. Recommendations

As reported and catalogued by CISA and the U.S. National Vulnerability Database, there are thousands of known vulnerabilities in OT/ICS machines and devices.

Threat actors continue to aggressively probe Enterprise/IT, OT, and IoT networks across the globe and are growing in capacity and sophistication of capabilities and enhanced TTPs.

To minimize risk and maximizing operational resiliency, critical infrastructure organizations should prioritize proactive defense strategies that include network segmentation, asset discovery, vulnerability management, patching, logging, endpoint detection, and threat intelligence. There is also a growing need for actionable asset and threat intelligence that can be used by different stakeholders within an organization such as IT teams, compliance officers and risk managers who may have different perspectives on security issues.

This includes:

- Deploying asset intelligence
- Using privileged access management
- Implementing the latest patches to VPN technology
- Using strong multi-factor authentication (MFA) not susceptible to vishing or SIM swapping
- Making frequent password changes
- Increasing employee training on vishing and overall social engineering

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

NN-SEC-RP-FULL-2023-2H-001