NOZOMI NETWORKS LABS

OT/IOT SECURITY REPORT

Unpacking the Threat Landscape With Unique Telemetry Insight

August 2023

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

Industrial and critical infrastructure security is at the forefront of decision makers' minds – from government leaders to CISOs to those on the front lines of the Russia-Ukraine War. With at least a dozen threat groups targeting the electric subsector globally, the fragility of sectors that underpin health and prosperity continues to be exposed.

Despite the fluctuating macroeconomic climate, the first half of 2023 continued to witness cyberattacks spanning hyper-connected facilities and operations like hospitals, manufacturing facilities, and transportation, and critical resources like energy and water.

This report features trend analysis leveraging open-source data and collated publicly available information and resources, as well as independent and unique telemetry data. We begin by reviewing the current threat landscape, the continuing trends of ransomware, and emerging trends like the advent of ChatGPT and targeting of the healthcare sector. We then expand on statistical analysis of recent attack patterns tracked through Nozomi Networks products: access vectors, malware types, and target characteristics. Finally, we dive deeper into independent research conducted via Nozomi Networks' globally distributed chain of passive IoT honeypots.

So far in 2023 Nozomi Networks has analyzed several attacks that can be categorized by industry and region. In this report, we summarize the most impactful events affecting OT and IoT cybersecurity and share unique insights into the current state of cybersecurity across various industries. Based on telemetry data shared by Nozomi Networks customers we are tracking a high volume of network scanning indications in water treatment facilities, cleartext password alerts across the building materials industry, program transfer activity in industrial machinery, OT protocol packet injection attempts in oil and gas networks, and more.

The number of vulnerabilities discovered in OT and IoT devices remains high, many of which are considered critical and/or easily exploitable. Increased process automation all over the world is creating new challenges for OT environments, especially where OT systems have limited security visibility and are increasingly expected to be or become interoperable with existing enterprise IT systems. The addition of new IoT deployments, various sensing capabilities, transient devices, additional networks and business integrations are also adding new attack vectors and expanding the traditional threat landscape.

2. The Threat Landscape

The first half of 2023 was full of OT/IoT cybersecurity events, many of which were continuations of trends we've seen in 2022. Ransomware continues to plague businesses of all sizes and sectors across the globe. Healthcare, energy, and manufacturing continue to be targeted by nation states, criminal groups, and hacktivists. Threat groups like REvil are now tinkering with the potential to combine autonomy, machine learning and natural language models into emerging technologies.

Meanwhile, newly discovered and disclosed CVEs in both hardware and software components are reported weekly, many of which impact multiple sectors that own and operate similar vendor systems and technologies.

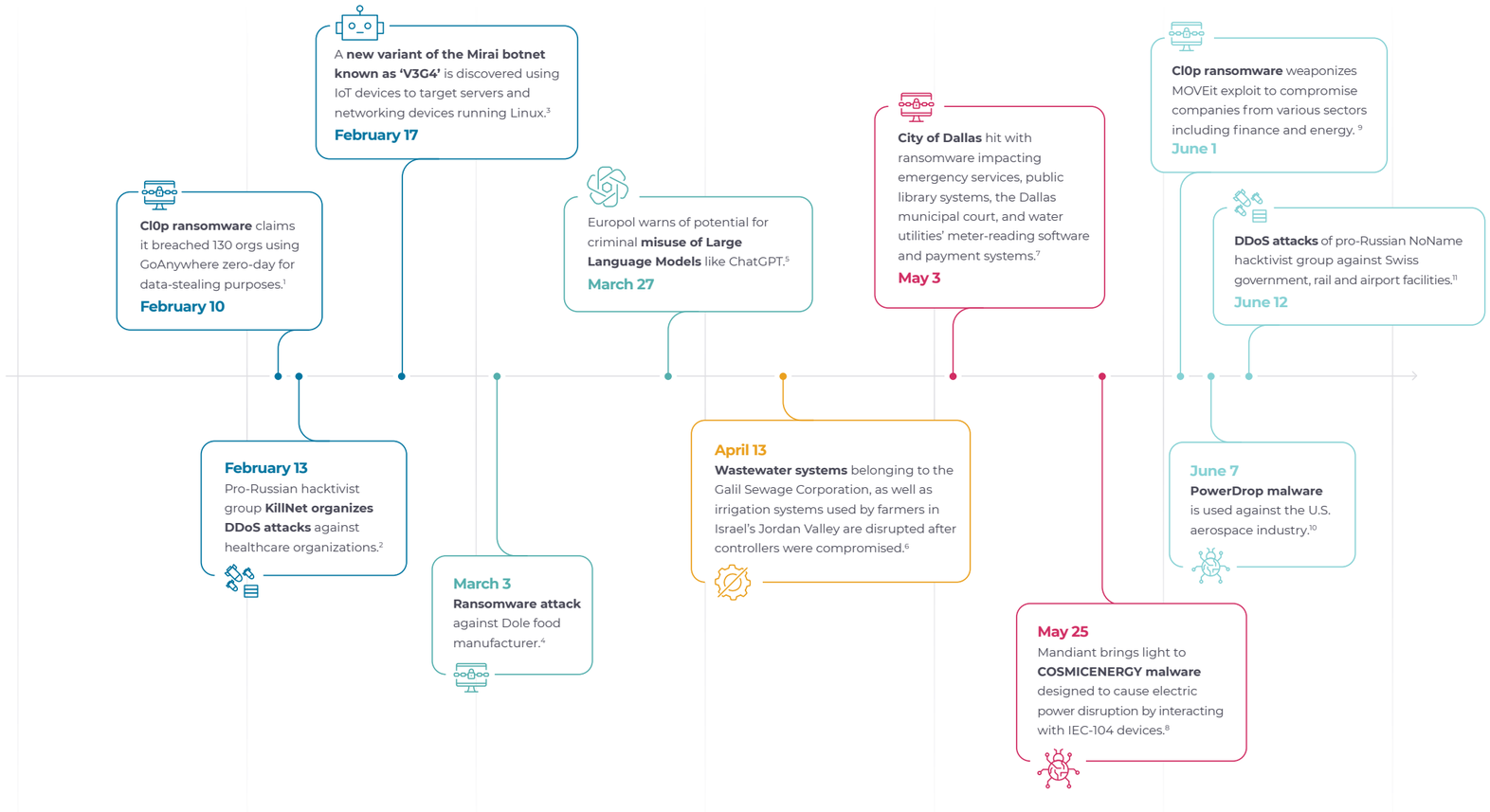
2.1 Timeline of Notable Events in the First Half of 2023

This timeline highlights several significant cyber events between January and June that have helped shape the current threat landscape.

Since the beginning of the year, we continue to see high-profile cyber activity from several types of threat actors, mainly featuring ransomware gangs deploying living-off-the-land techniques. These techniques are easily accessible, capable of evading detection, highly adaptive, and supportive of automation.

We see manufacturing, energy, healthcare, water and wastewater impacted, as well as government and city services disrupted. In addition to ransomware, Distributed Denial of Service (DDoS) attacks emerged as well as new variants of the 2016 Mirai botnet. Industrial control systems were directly impacted in at least three of the incidents in this time period.

Governments around the world have been working to enhance cybersecurity legislation and critical infrastructure policy at the national level in the first half of the year, including the U.S. National Cybersecurity Strategy and its subsequent implementation plan, the European Union NIS 2 Directive, and the Security of Critical Infrastructure Act in Australia.



As critical infrastructure attacks continued to make news headlines in the first half of 2023, governments around the world were adding enhanced cybersecurity legislation and critical infrastructure policy at the national level. New attention is being paid to securing sectors that are integral to the economy, health and human safety, and national security.

The January 2023 NIS 2 Directive in Europe requires national policy creation by each EU Member State to strengthen cybersecurity and capabilities to prevent, detect, and respond to security incidents in critical sectors.

The U.S. National Cybersecurity Strategy released in March 2023 specifically focuses on defending critical infrastructure. It introduces new regulation for cybersecurity across critical infrastructure sectors and encourages security by design in the development of vendor products.

In the same month, Australia amended the 2018 Security of Critical Infrastructure (SOCI) act with new obligations for strengthening the security and resilience of critical sectors and assets.

In May 2023 the U.S. Cybersecurity and Infrastructure Security Agency (CISA) also released a white paper, "Highlighting R&D Needs and Strategic Actions for Enhancing the Resilience of Critical Infrastructure". The paper recommends a dozen strategic actions for holistic implementation by research partners for a more integrated, empirical, and user-informed approach to federal research, development, and innovation.

The suggestions cover (1) An integrated analysis of consequences and risk reduction decision factors for critical services that depend on cyber-physical infrastructure systems; (2) An understanding of the societal dimensions of enhancing the resilience of cyber-physical infrastructure systems; and (3) User-engagement in cyber-physical infrastructure research to translate resilience knowledge into effective action at the local and regional level.[12]

As cyber threats to critical infrastructure continue to rise and evolve, governments around the world are stepping up their efforts to establish stronger cybersecurity standards and speed efforts to strengthen security and resiliency.

Enhanced Cybersecurity Legislation and Critical Infrastructure Policy in the First Half of 2023

2.2 Ransomware Updates

Ransomware activity remained strong in the first half of 2023, with dozens of threat actors claiming hundreds of new victims based on the publicly disclosed incidents we reviewed. This section covers the three most active and concerning groups for critical infrastructure with commentary on their most recent attacks.

2.2.1 Cl0p Gang

At the time of writing, the most impactful ransomware event this year was orchestrated by the Cl0p ransomware gang (also known as TA505). Cl0p continues to exploit the CVE-2023-34362 vulnerability in MOVEit Transfer software, with the first known exploits deployed at the end of May. Since then, the list of victims has grown daily and includes U.S. government agencies, oil and gas giants, several banks, media companies and universities. The ransomware group has been adding new victims at a rate of 13-14 victims per day[13] and seems to be far from finished. In February, the same group compromised multiple companies targeting a different vulnerability in GoAnywhere software. On June 16, the U.S. government offered a US $10 million reward for information that could link the gang to critical infrastructure attacks conducted while operating under the direction of any foreign government.[14]

2.2.2 LockBit Group

LockBit has been one of the most active and prolific Ransomware-as-a-Service (RaaS) groups in 2022 and 2023. Since 2020, LockBit has extorted more than $91 million from the U.S. alone. Their activity has triggered CISA and its U.S. and international partners to release a joint advisory with tips to help organizations understand and defend against LockBit attacks.[15]

The LockBit RaaS is so widespread that it accounts for 10% to 25% of all ransomware attacks, depending on the country.[16] LockBit's threat actors have consistently refined and adapted their ransomware strain to infiltrate Linux, VMware ESXi, and Apple macOS systems. This persistent and swift innovation serves as a stark reminder that organizations must maintain constant awareness and exercise vigilance to minimize potential risks.

2.2.3 ALPHV/BlackCat Group

The ALPHV group, also known as BlackCat, is another popular RaaS that made headlines in early 2022 when the FBI covered them in a Flash Alert as the first ransomware group to successfully compromise its victims utilizing RUST as a main programming language.[17]

ALPHV recently became the second most active ransomware group (accounting for ~14% of total ransomware victims). This ransomware is highly effective and constantly updated. Their list of publicly disclosed victims includes an online news aggregator and technology, plastics and critical infrastructure component manufacturers among others.

2.3 Healthcare Sector Spotlight

Across the healthcare sector, cyberattacks are increasing in frequency while the attack surface for facilities and organizations continues to grow. Healthcare has become the third most targeted industry globally, with weekly attacks increasing by 74% from 2021 to an average of 1,463 attacks per week, according to Check Point Research.[18]

Their research also found that criminal ransomware groups are becoming smaller and more agile, and getting better at evading law enforcement attempts to hold them responsible for attacks.

Healthcare is an attractive target for threat actors not only because of lucrative business models, but the growing number of connected devices and assets involved in their operations. It's worth mentioning that the vast majority of healthcare organizations rely heavily on legacy equipment (outdated or no longer maintained), which is by far the highest risk factor for the industry.

According to IBM Security – a Nozomi Networks partner – the average data breach in the sector costs $10.1 million, often the result of third-party vendor access. With thousands of different vendors, attacks in this space continue to be an "when, not if" paradigm. There are hundreds of publicly disclosed product vulnerabilities impacting the sector, and a growing number of IoT devices known to be at risk.[19]

While the number of vulnerabilities specific to the healthcare sector spiked in the second half of 2022, pushing healthcare into the top 5 list

HEALTHCARE SECTOR STATS

3rd
most targeted industry globally

74%
increase in weekly attacks from 2021

1,463
average attacks per week

$10.1 million
average data breach cost

of vulnerabilities in our previous report, so far this year we've seen a decline in the number of healthcare vulnerabilities reported (dropping to 11th place). However, 83% of the reported vulnerabilities' risk levels were high or critical.

STATS

83%

of the reported vulnerabilities' risk levels were high or critical

In an attempt to keep pace with this rapidly growing attack surface, the U.S. Food and Drug Administration passed new legislation that took effect in March requiring medical device manufacturers to take measures to include security by design or add cybersecurity protections to their products before they are brought to market.

This year Nozomi Networks Labs is expanding its healthcare research practice.

Early findings have uncovered some concerning – yet very common - issues around poor cybersecurity practices, when it comes to both device and communication security.

Critical medical equipment tends to be poorly hardened and often its integration into the rest of the network dramatically raises the level of risk for the whole organization.

Basic cybersecurity hygiene is often overlooked leading to a sharp increase in the risk of healthcare devices being leveraged as entry points or being rendered unavailable or unreliable.

NOZOMI NETWORKS BLOG

Ensuring Cybersecurity of Medical Devices: What Changed in the FD&C Act?

The Omnibus amendments to the FD&C Act went into effect on March 29, 2023. The new legislation authorizes the Food and Drug Administration (FDA) to require medical device manufacturers to take measures to include security by design or add cybersecurity protections to their products before they are brought to market.

Read More ›

2.4 The AI Revolution

In our last research report covering the second half of 2022 we referenced ChatGPT, predicting how it may be used with malicious intent. While technology still does not pass the Turing test, as Nozomi Networks CTO Moreno Carullo pointed out in his March blog post,[20] it has evolved at a very fast pace. This has triggered events like a Future of Life Institute open letter signed by many AI experts requesting AI labs to "immediately pause for at least 6 months the training of AI systems more powerful than GPT-4."[21]

It's often very easy to circumvent the "guardrails" put in place by AI model creators. However, the concerns shouldn't stop at how these platforms could be manipulated. They should also include the reliability of the data provided by AI-based tools, and the potential to poison neural models. LLMs (Large Language Models, like ChatGPT, Google Bard, etc.) are being increasingly used by malicious actors to distribute malware disguised as OpenAI-powered apps or to generate various data required in different attack stages.[22]

The ever-growing community working on generative AI models and exploring their capabilities makes these tools widely available to the general population. These new AI systems can be used to automate processes and help cybersecurity defenders with an ever-growing variety of tasks including:

- Phishing email detection,[23]
- Code generation and debugging,[24]
- Grammar reviews,
- Text translations, and more.

With these advances in research and innovation, more and more companies are employing AI tools to automate workflows. As an example, hundreds of industrial and critical infrastructure organizations today benefit from machine learning capabilities in Nozomi Networks solutions to automate and speed alerting and reporting for stronger defenses.

In June, we introduced Vantage IQ, the industry's first AI rules-based analysis and query engine. It replicates learned experiences of seasoned security analysts and automates the and time-consuming tasks of reviewing, correlating, and prioritizing the enormous amount of collected network, asset, and alert data to provide meaningful insights into real threats and how they should be addressed. In this case, AI supports security teams with more context to focus on priority issues and do their jobs more efficiently.

Unfortunately, AI systems are also being used by threat actors. Earlier this year Europol organized several workshops to explore ways criminals are abusing the large language models and issued public warnings[25] around the following three criminal areas:

- **Fraud and social engineering**: LLMs' ability to draft highly realistic text makes it a useful tool for phishing purposes. The ability of AI

models to reproduce language patterns can be used to impersonate the style of speech of specific individuals or groups. This capability can be abused at scale to mislead potential victims into placing their trust in the hands of criminal actors.

- **Disinformation**: LLMs excel at producing authentic sounding text at speed and scale. This makes the model ideal for propaganda and disinformation purposes, as it allows users to generate and spread messages reflecting a specific narrative with relatively little effort.
- **Cybercrime**: In addition to generating human-like language, LLMs are capable of producing code in a number of different programming languages. For a potential criminal with little technical knowledge, this is an invaluable resource to produce malicious code.

If you want to leverage AI technologies, it is extremely important to be aware of the security implications and reduce risk.

We recommend using local deployments over online tools where possible, and sanitizing every input when a local deployment is not possible. Remember that the integrity of the model's output should be the primary concern.

NOZOMI NETWORKS BLOG

ChatGPT-4: AI's Evolving Capabilities and Consequences for Cybersecurity

ChatGPT, the OpenAI chatbot, has taken the tech world by storm.

This interesting technology responds to queries and exchanges information back-and-forth in a manner that is almost human.

With the release of ChatGPT-4, the speed at which AI is evolving has practitioners wondering what the impacts will be to cybersecurity.

Read More ›

3. The Vulnerability Landscape

Being aware of the landscape of vulnerabilities affecting OT devices manufactured, integrated, and maintained in critical infrastructure around the world can help asset owners make informed decisions when organizing protection. In this section we analyze data from all ICS advisories released by CISA[26] between January 1 and June 15, 2023.

During this period, CISA reported 171 new advisories detailing 641 vulnerabilities affecting various products from 62 different vendors, a slight drop compared to 70 in the previous period.

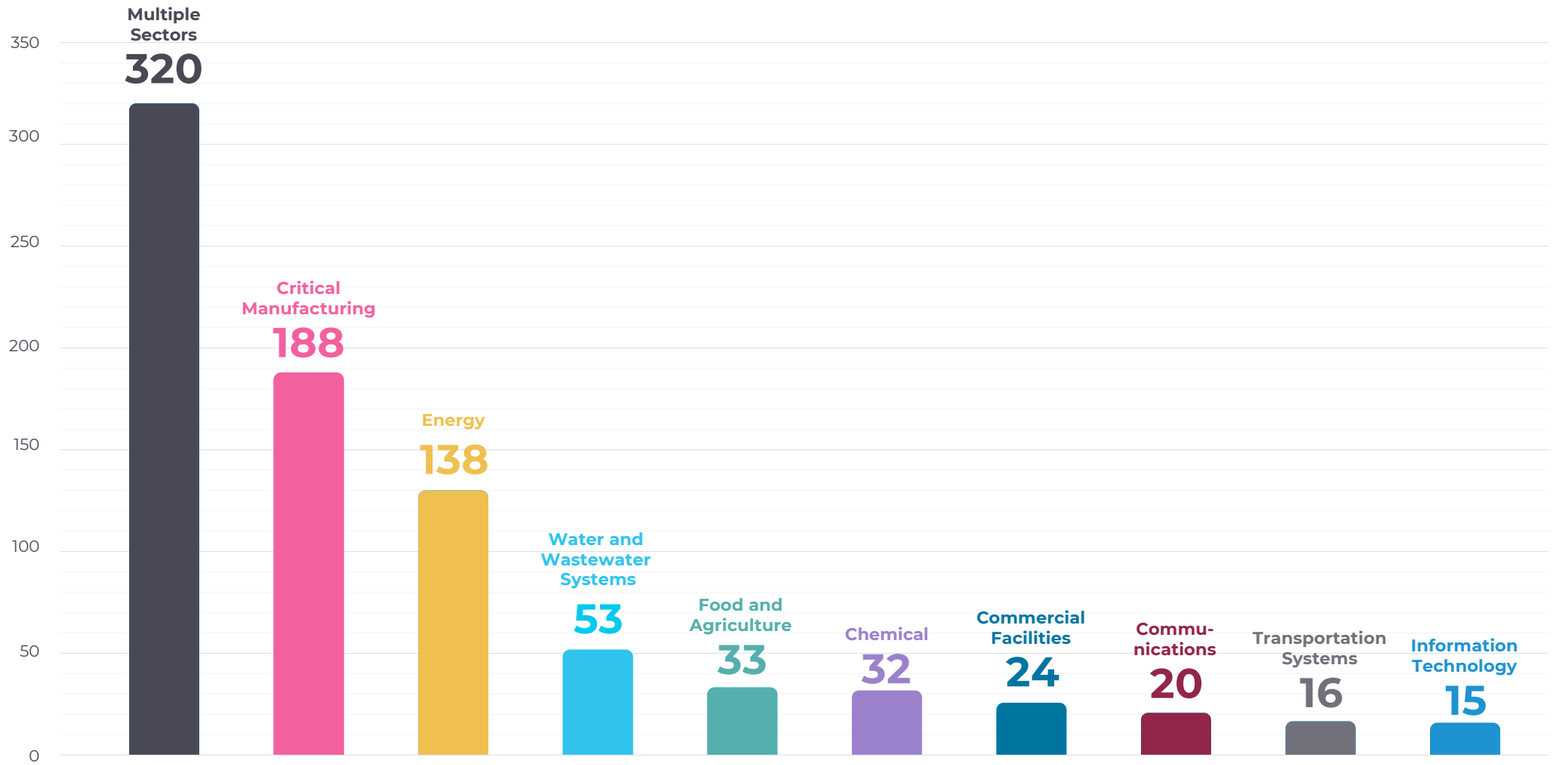
Let's get into the details.

3.1 Number of CVEs Released by Sector

Looking at the top 10 industries affected by disclosed ICS-CERT vulnerabilities, critical manufacturing continues to be the most vulnerable standalone sector.

Energy comes in second, followed by Water and Wastewater. Two new vulnerable industries moved into the top 5 – Food & Agriculture and Chemicals. Transportation vulnerabilities dropped to ninth place, from a previous position in the top 5. And, while Healthcare vulnerabilities came in fourth in our previous six-month reporting period, in the first six months of 2023, healthcare dropped out of the top 10 ranking.

It's important to note that half of all vulnerabilities reported so far this year fell into CISA's Multiple Sector category – meaning they involved technologies used by more than one sector.



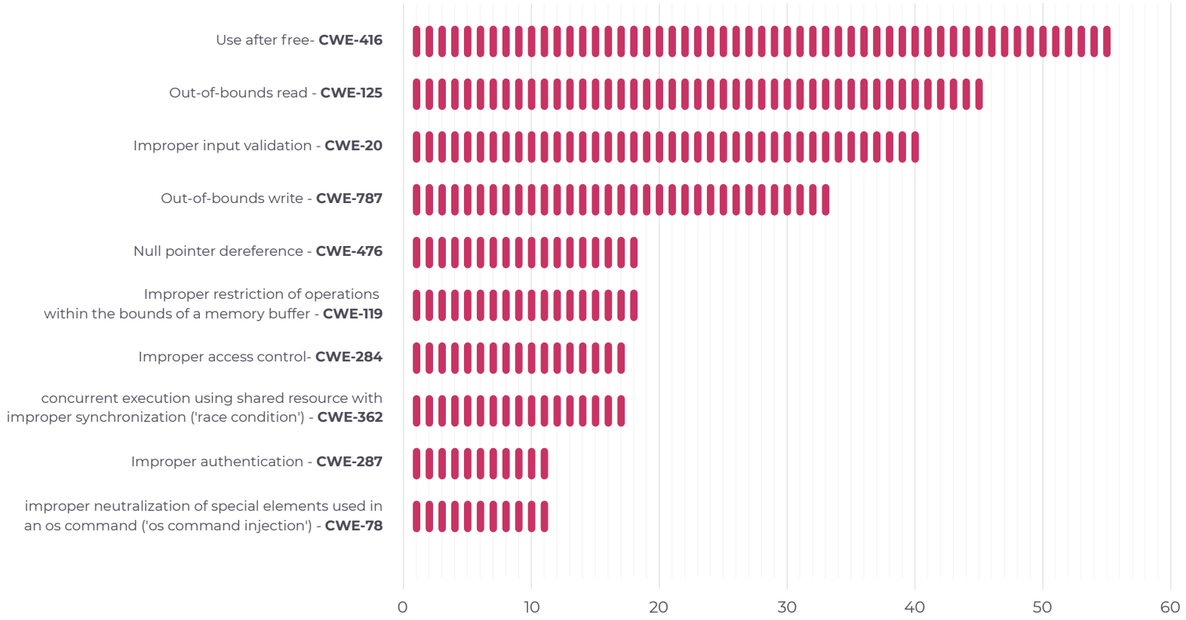
3.2 Number of CWEs Associated with CVEs

In this section we explore the top Common Weakness Enumerations (CWEs) associated with CVEs released in the first half of 2023, between January 1 and June 15. Becoming familiar with these common software and hardware security flaws can give organizations insights into how to better secure their networks.

Surprisingly, a dark horse – Use-After-Free – was the most frequently discovered CWE during this reporting period. Also known as a dangling pointer vulnerability, it is associated with the incorrect use of dynamic memory during program operation. If a program continues using the pointer after freeing memory, a threat actor can use the error to hack the program.

It is interesting to see Use-After-Free in the top spot because historically it has been a less common CWE. Generally, it is more difficult to spot Use-After-Free issues compared to classic buffer overflow or SQL injection vulnerabilities. While we don't have an obvious explanation for this occurrence, it could suggest that the capabilities of security products overall have improved, and security researchers can now focus on more complex CWEs.

Finally, it is worth noting that both Out-of-Bounds Read and Out-of-Bounds Write operations remained in the top CWEs. Both are commonly associated with buffer overflow vulnerabilities. And improper input validation may lead to multiple different attacks, for example, SQL injections.



4. Attack Statistics from OT Environments

In this section, we provide original analysis of Nozomi Networks monitoring telemetry, provided by customers participating in our anonymized data sharing project.

Thanks to those who have opted in to securely share their data, we are able to aggregate detection information 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 2023.

4.1 Commonly Detected Malware Categories

In addition to product alert categories, we explore what malware categories were most commonly detected by Nozomi Networks customer deployments across Enterprise/IT, OT, and IoT environments as well as cross-domain entries seen during the period of January 1 to June 15, 2023.

The results below indicate the total number of unique alerts raised in our customers' environments, categorized by network domain type.

For Enterprise/IT environments, the generic "Trojan" category remains prevalent, as it was in our previous reporting period. Trojan malware is often used as an umbrella category for many types of associated threat activities commonly used by adversaries. The category may represent threat activity which incorporates the functionality of multiple malware categories or may be used when it is too resource intensive at that time to properly identify a separate category.

"Dualuse" is another commonly detected category as it covers tools which, depending on the use case, may have a legitimate use for an administrator in the environment and/or could be used maliciously by a threat actor to compromise an environment. As an example, PsExec, which is often used by system administrators to control a computer from a remote location, falls in the Dualuse category because it is also commonly misused by attackers for lateral movement.

"Worm" activity jumped to the third highest category of active malware – up from seventh place in the previous six months. Finally, "Ransomware" remains a frequently witnessed malware category across Enterprise/IT domains, causing significant damage to normal business operations all over the globe.

In OT network domains, Denial-of-Service (DOS) malware activities lead in frequency, as one of the most prevalent attacks against OT systems. This is followed by the Remote Access Trojan (RAT) category commonly used by attackers to establish control over compromised machines as it provides flexibility in the next stages of the attack. Six months ago, these two categories also lead the chart with RAT being the top choice of attackers.

In IoT network domains, similar to what we saw in our previous report, Distributed Denial of Service (DDOS) threats are also the top

threat because this malware category has become easy to monetize. It is easier for DDOS attacks to be leveraged at scale given the size of IoT deployments. Despite each device or sensor generally being weak in terms of computational power, the nature of IoT is highly distributed where nodes can be automatically compromised without the need for an attacker to compromise one after another. Many IoT botnets like Gafgyt and Mirai capitalize on this functionality to disrupt IoT networks and devices for extortion attempts without creating specialized ransomware.

When analyzing cross-domain malware, phishing alerts are the most prevalent threat activity falling under multiple domains, commonly used to steal sensitive information and establish initial access, sometimes deploying malware to infect targets.

Most Commonly Detected Malware Categories

July to December 2022

Affected Environment	Malware	Number of Detections
Enterprise	Trojan	**8,343**
Enterprise	Dualuse	**6,058**
Enterprise	Worm	**1,995**
Enterprise	Ransomware	**133**
Enterprise	RAT	**34**
Enterprise	DDoS	**22**
Enterprise	Infostealer	**10**
Enterprise	Exploit	**2**
Enterprise	Miner	**1**
OT	DoS	**199**
OT	RAT	**27**
OT	Trojan	**2**
IoT	DDoS	**3**
IoT	Exploit	**2**
Multi	Phishing	**26**
Multi	Dualuse	**25**
Multi	Webshell	**18**
Multi	RAT	**7**
Multi	Scanner	**2**
Multi	Trojan	**1**

4.2 Types of Intrusion Alerts

In this section we look at the top 20 alerts by alert-type detected by Nozomi Networks products between January 1 and June 15, 2023, from most to least detected.

Detection of network scanning activity was the most frequent alert type. There are many reasons for this including ones that aren't nefarious. Network scanning is often very noisy, commonly sending many different payloads to multiple devices and machines. Additionally, many companies actively scan their own environment to search for vulnerabilities. This is great news that companies appear to be investing in more resources for visibility compared to our previous report when this type of alert wasn't even in the top 10.

The second and third most triggered alerts unfortunately reveal an ongoing trend related to insufficient credential management, a similar ranking to six months ago. We continue to detect weak credentials being used and insecurely handled (for example, passed in plain text during the authentication process), making it easier for attackers to guess or sniff them by intercepting parts of the network traffic. This activity can be correlated with multiple triggered alerts for unsuccessful logins and access denied events generally representing brute-forcing attempts using, among others, standard and stolen credentials.

Together, insufficient credential management and alerts for unsuccessful logins and access denied events often indicate potential brute force password attacks. Other alerts listed above include certain activities that may indicate a risk to the OT environment like protocol packet injections, malformed traffic, and unsupported function requests – where certain machines receive function codes not associated with their OEM configuration specifications.

Top 20 Most Critical Types of Intrusion Alerts

January 1 to June 15, 2023

Network Scan	**27 %**	New link	**3 %**
Cleartext password	**12 %**	TCP flood	**2 %**
Weak password	**8 %**	New target node	**2 %**
Program transfer	**7 %**	Malformed Network packet	**1 %**
Malformed traffic	**6 %**	Missing variable request	**1 %**
OT protocol packet injection	**5 %**	TCP SYN flood	**1 %**
Packet rule match	**5 %**	Multiple unsuccessful logins	**1 %**
Multiple Access Denied events	**4 %**	Unsupported function request	**1 %**
Program download	**4 %**	Weak encryption	**1 %**
Invalid IP	**4 %**	Variable flow anomaly	**1 %**

Intrusion alerts not in the top 20 account for 4% of all detections.

4.3 Industry Insights

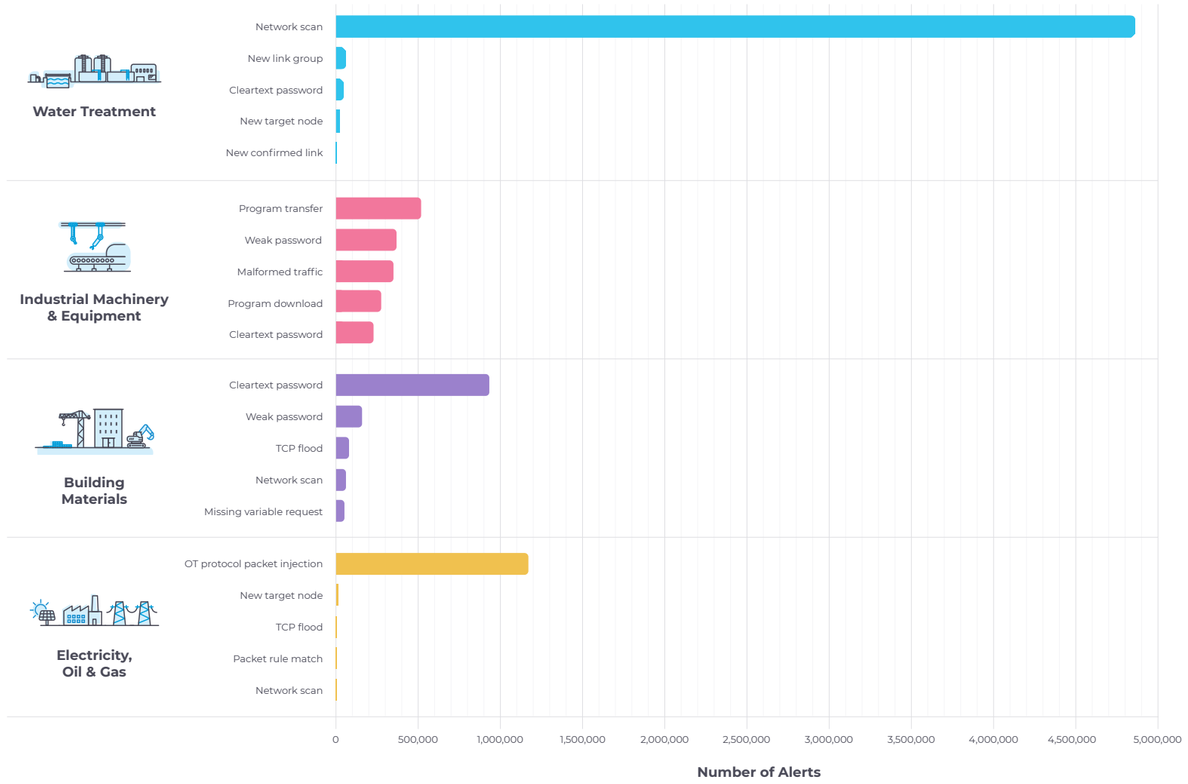
This is a new section not previously featured in our security research reports. With the advancement of our telemetry analysis across customer environments, we are able to see the distribution of unique alerts by industry.

The most triggered alerts vary depending on the industry. Water Treatment facilities witnessed more generic network scanning typically associated with authorized scanning or threat actor probing. Meanwhile, customers in Oil and Gas were more likely to experience alerts related to OT protocol packet injection, which involves a correct protocol packet injected in the wrong context. For example, a correct protocol message could be sent in the wrong sequence. Taken in sum, many sectors share similar common alert types like poor credential management, cleartext password identification, and TCP flood alerts.

At face value it may be difficult to prioritize the list of relevant alerts, because in order to do it, analysts must compare the significant potential new target node – a node on the network that is not known and has not yet sent any data – to the program download alert – when an OT device program has been downloaded from another host. To help administrators solve this challenge, the Nozomi Networks platform automatically calculates a customized security profile level for these types of alerts and assigns a base risk score. Our alerts Playbook also provides suggested actions for each type of alert listed.

Here are the results for the most commonly detected malware types by industry, with the corresponding number of alerts and their type.

Average Number of Alerts Per Customer, by Industry

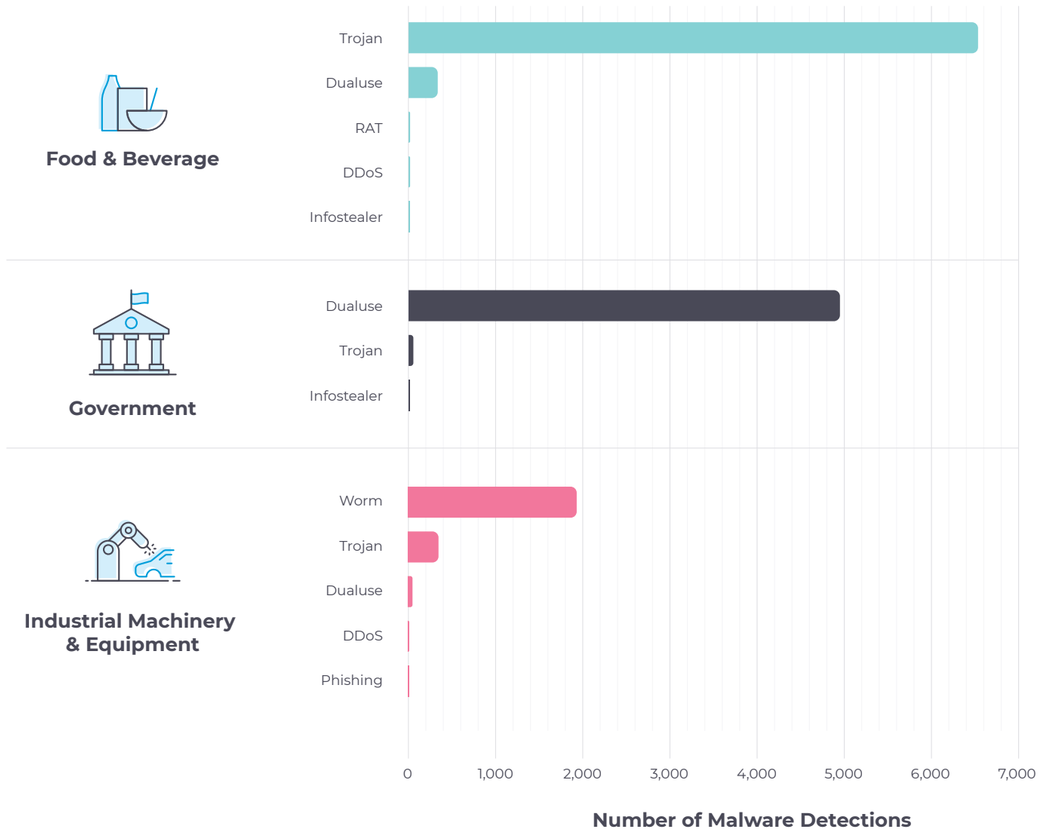


Depending on the industry, the distribution is slightly different with the most common Trojan and Dualuse categories commonly found in network domains across industries.

As we saw in the overall alert types analyzed, DDoS attempts are constant threats for customer environments. In addition, Infostealer malware – designed to steal victim information and passwords – appears a number of times in Food & Beverage environments, as we saw in the Enterprise/IT distribution above.

This could potentially indicate threat actors probing Food & Beverage environments to assess access vectors, map networks, and possibly plot attack paths. As we know from the last decade of OT and IoT security, the vast majority of cyber incidents continue to begin in the Enterprise/IT domain.

Most Commonly Detected Malware Types by Industry



4.4 Regional Insights

This is another new section not featured in previous Nozomi Networks security research reports. The country snapshots below provide analysis of telemetry data from the first half of 2023 from multiple sectors investing in cybersecurity for OT and IoT.

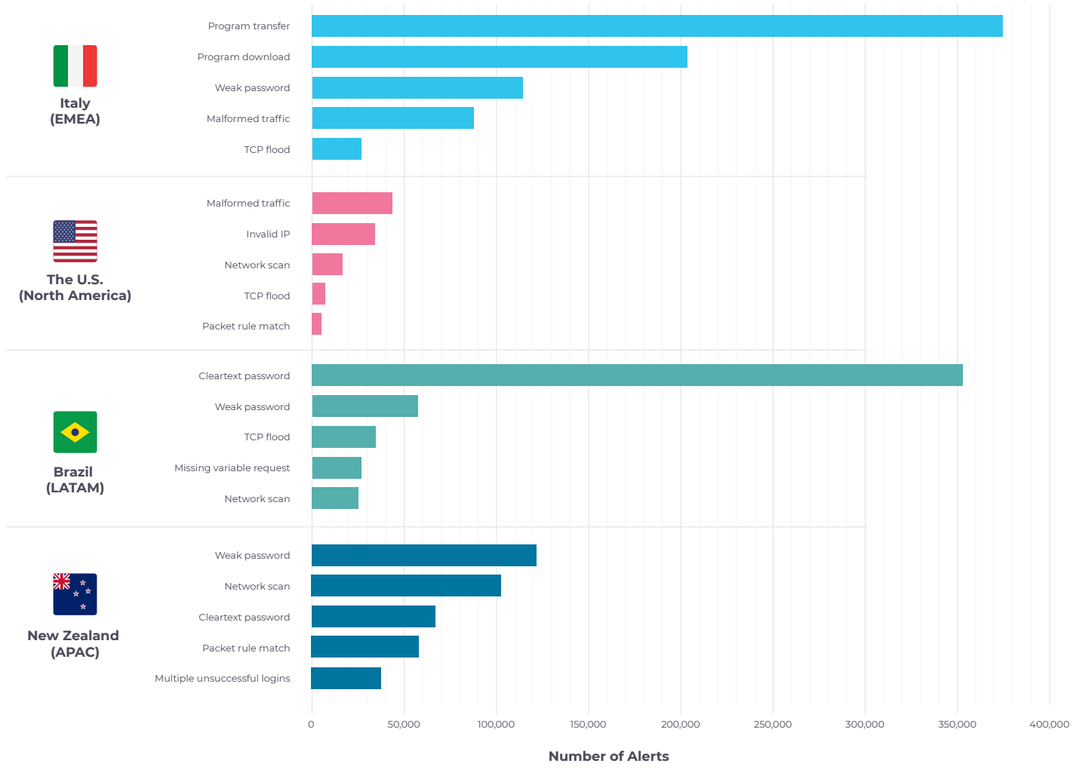
It is important to note that the number of alerts per country does not necessarily indicate that the following countries are the most frequently targeted; the data also reveals countries where owners and operators have invested in increased network visibility in their environments and regularly gather data to perform security audits. Below are snapshots of the highest average number of alerts per customer from one country per region where the Nozomi Networks solution is deployed.

The listed alert types cover many types of rule detections, representing network events that could potentially represent a threat to the organization.

We can see that the same alert types discussed in the global alert overview (Section 4.2) lead the charts for each country, though on a different scale. Some repeat offenders like insufficient credential management are more common in some countries, while low-level alerts like Program transfer and Malformed traffic are common in others with more visibility into OT environments.

Among other factors, it is dependent on the inventory and diversity of products that OT industries use in different countries.

Most Commonly Detected Alerts Per Country



5. The IoT Botnet Landscape

In this chapter we analyze data collected by Nozomi Networks Labs' globally distributed chain of passive IoT honeypots. These honeypots are independent research instances and not located in either Nozomi Networks' or our customers' environments.

The devices they emulate can be found in commercial and industrial operations around the world. While past reports have previewed mainly the attack patterns deployed against our distributed honeypots, the following section also adds statistics related to the malware samples collected by them. This unique data can help security teams get a better understanding of the threats they face, validate their existing defense strategy and approach, and inform future decision-making.

5.1 Attack Source Locations

Between January 1 and June 15, 2023, we counted the total number of unique IP addresses from the origins of the attacks against our honeypots and mapped them to countries where the associated servers are located.

Figure 1 shows that over the last six months, devices in China, the U.S., South Korea, Taiwan and India were most frequently leveraged by threat actors to initiate attacks. This indicates that these locations have vulnerable systems which can be exploited by cyber criminals, allowing them to spread their malicious code quickly and easily. The activity was fairly consistent with our analysis in the second half of 2022, however activity dropped 28% over the previous period in South Korea and increased 6% and 106% in Taiwan and India respectively.

In the majority of 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. For example, many of the IP addresses originating from machines located in China, the U.S. and South Korea may also be attributed to the increased adoption of smart, connected devices throughout many sectors in these countries, resulting in a wider attack surface – higher numbers of machines that can potentially be compromised.

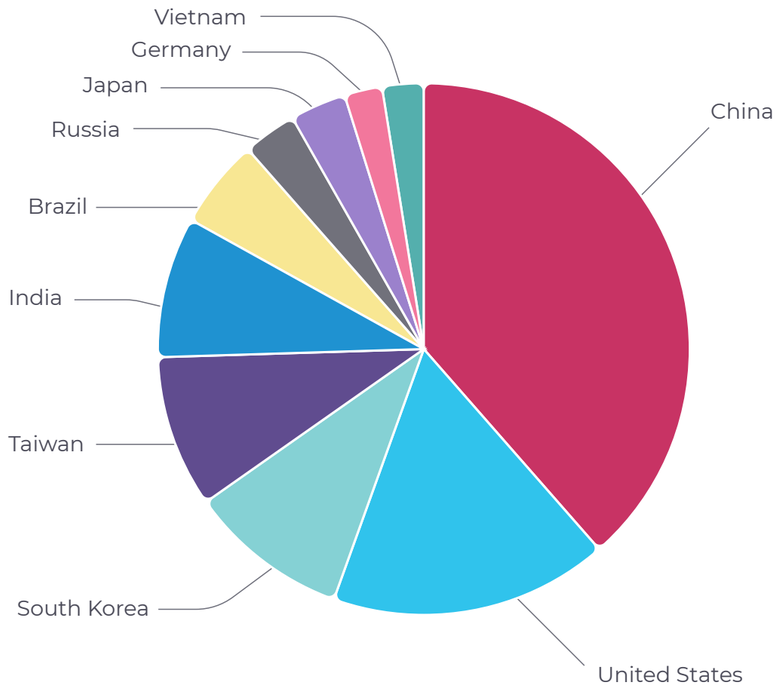


Figure 1: Top countries where compromised devices were used to execute attacks, January-June 2023.

5.2 Number of Unique Daily Attacker IPs

Our honeypots collected 69,591 unique attacker IPs in the first half of this year. On average we tracked 813 unique attacker IPs daily and our highest attack day spiked at 1,342 on May 1. This data is quite interesting as it indicates how many unique machines were attempting to attack our honeypot infrastructure daily.

We can see how the numbers continuously fluctuate over time, indicating the changing landscape of compromised machines with some machines being cleaned up and new ones being added to botnets.

STATS

69,591
Unique attacker IPs in the first half of 2023

813
Average unique Attacker IPs daily

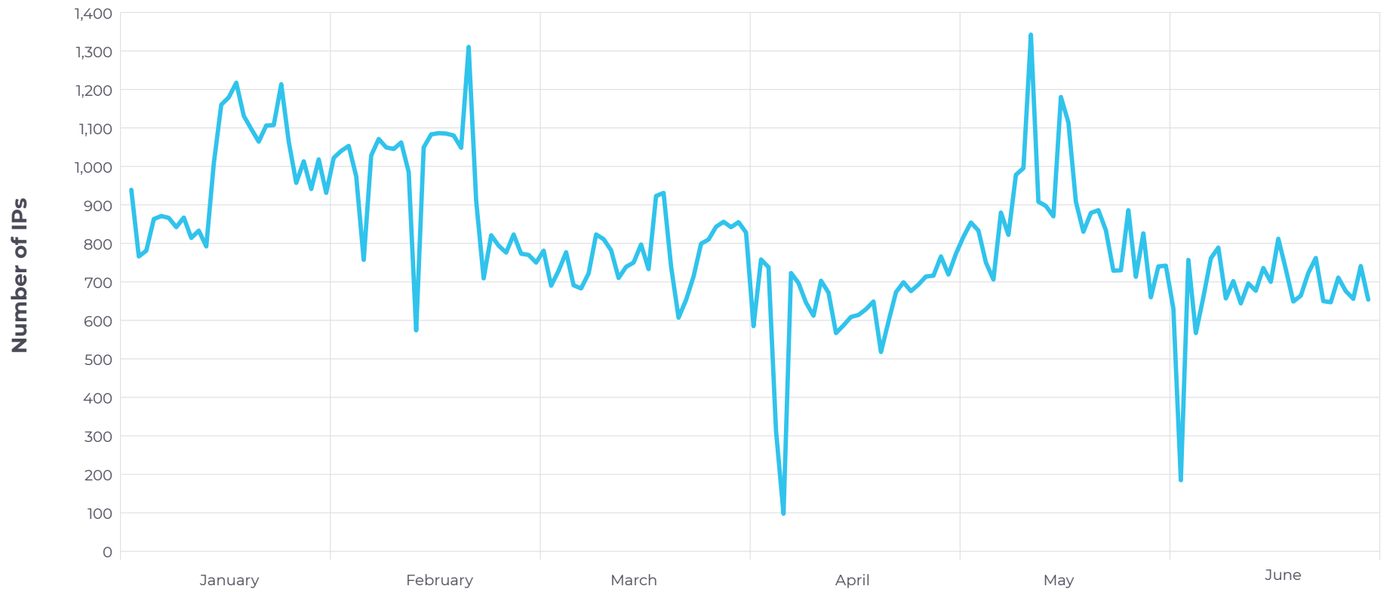


Figure 2: Unique attacker IPs, January-June 2023.

5.3 Top Credentials Used

Brute-forcing known credentials remains a popular technique to gain access to systems to hijack remote management of devices using protocols like SSH and Telnet.

Default credentials are one of the main ways threat actors gain access to IoT. Because many companies neglect to change their default passwords, threat actors use default credentials so that their access is not easily detected by network security systems. Figure 3 shows the top default usernames and passwords that threat actors use to gain initial access.

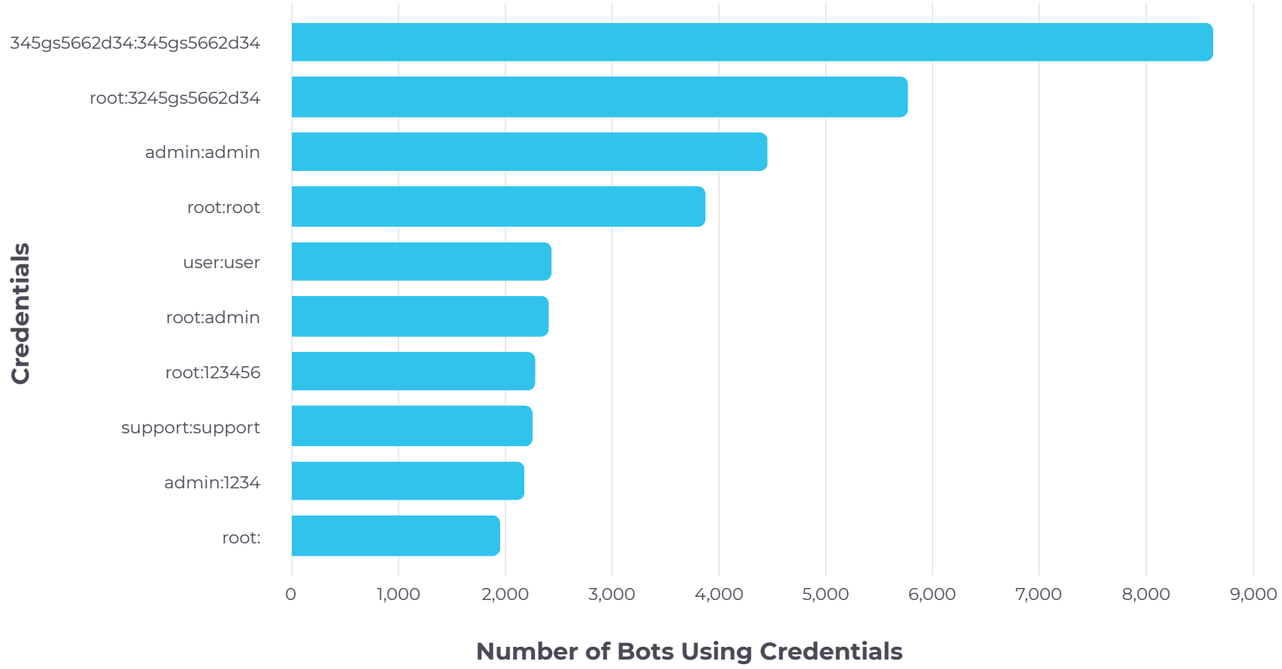


Figure 3: Top credentials used, January-June 2023.

5.4 Top Executed Commands

Following initial access, threat actors execute commands on a system that will allow them to maintain persistence and escalate privileges. Figure 4 shows the top executed commands from January through June of this year.

Some of these commands are generic and are used to get to the right shell or admin terminal. Others are quite interesting – featuring a hardcoded public SSH key that attackers are adding to a list of "trusted keys," such as the fifth most popular command. Trusted keys are used to maintain persistent access, providing a way to connect via SSH to the compromised machine later.

INSIGHTS

Because some of the commands are too long to be properly displayed on the diagram, here is the top 10 list in full:

1. enable
2. sh
3. shell
4. system
5. "cd ~ && rm -rf .ssh && mkdir .ssh && echo ""ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUanUV9tJ2/9p7+vD0EpZ3Tz/+0kX34uAx1RV/75GVOmNx+9EuWOnvNoaJe0QXxziIg9eLBHpgLMuakb5+BgTFB+rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEmPecjdySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCGPK5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujvcD9iUKQTTWYYjIlu5PmUux5bsZ0R4WFwdIe6+i6rBLAsPKgAySVKPRK+oRw==mdrfckr"">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~"
6. "cd ~; chattr -ia .ssh; lockr -ia .ssh"
7. "dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s"
8. "/bin/busybox BOTNET"
9. q
10. linuxshell

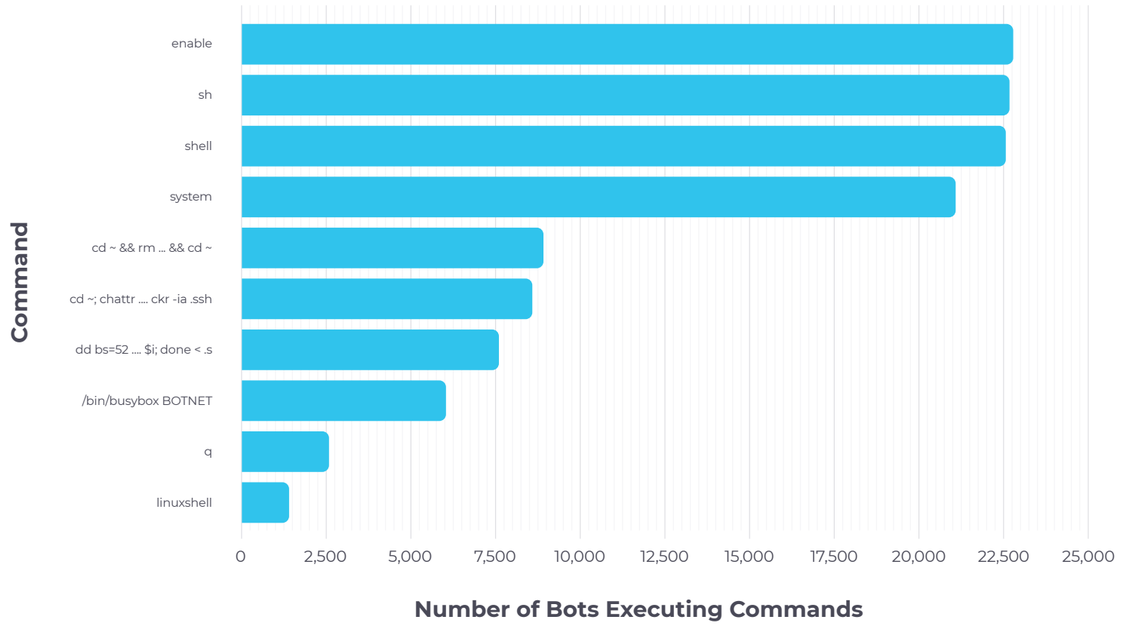


Figure 4: Top executed commands, January-June 2023.

5.5 Top Payload File Types

This is another new section of our report, where we analyze data related to the malicious payloads our honeypots were able to collect over this period of time.

First, let's look at the distribution of samples by their file types. 32-bit ARM architecture remains the most popular architecture targeted by attackers focusing on IoT environments, which is not surprising as lots of smart devices are based on it. 32-bit ELF payloads are the most common there as it is a main executable file format for multiple RISC architectures powering IoT devices. According to our data, most of the executable payloads were written in the programming language C/C++ for performance reasons. Overall, it is important to make sure security engineers involved in protecting IoT environments are comfortable analyzing ARM samples in general.

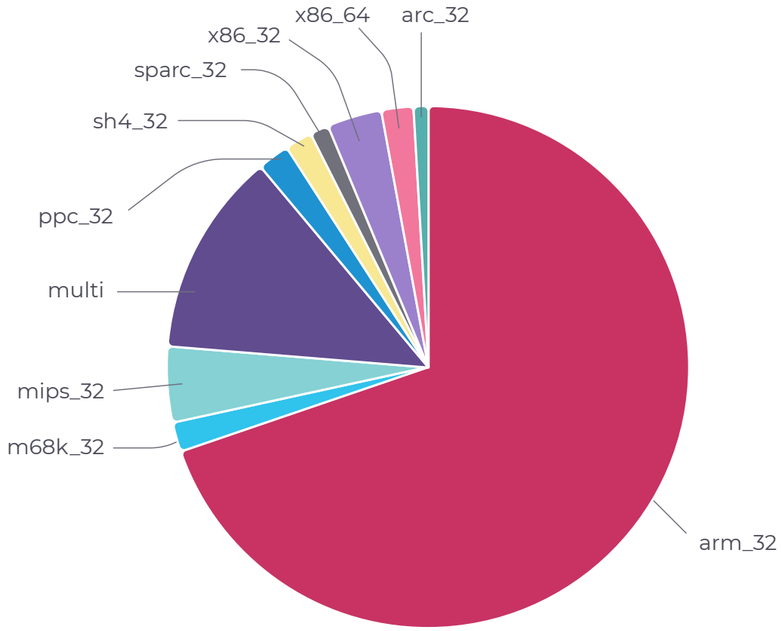


Figure 5: Top architectures supported by malware payloads, January-June 2023.

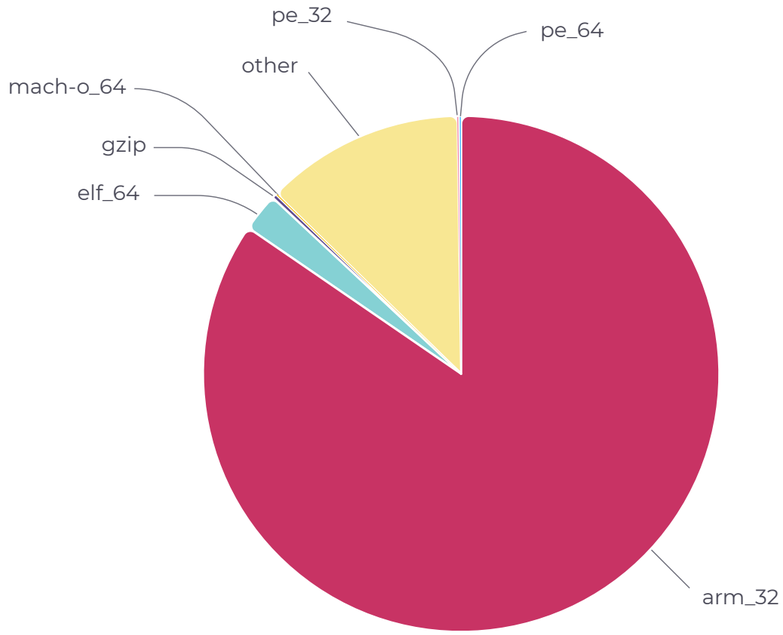


Figure 6: Top file types of malware payloads, January-June 2023.

5.6 Top Payload Packers

Next let's take a deeper look at collected binary payloads and see if they have been packed or not in order to complicate the analysis and detection process. Unlike Windows, the choice of open-source packers remains small for ELF files, which results in attackers either not using any, or relying on the well-known UPX solution.

Digging deeper, we can see that the majority of attackers still use the old and venerable version of UPX 3.94 while at the time of writing this report the latest release version is UPX 4.0.2. However, it is still important to ensure that your malware analysis automation tools incorporate the latest version of UPX to be able to correctly handle all of the samples. Additionally, at the industry conference S4x23 Nozomi Networks Labs released an open-source tool that can be used to automatically fix corrupted UPX structures and enable easy unpacking.[27]

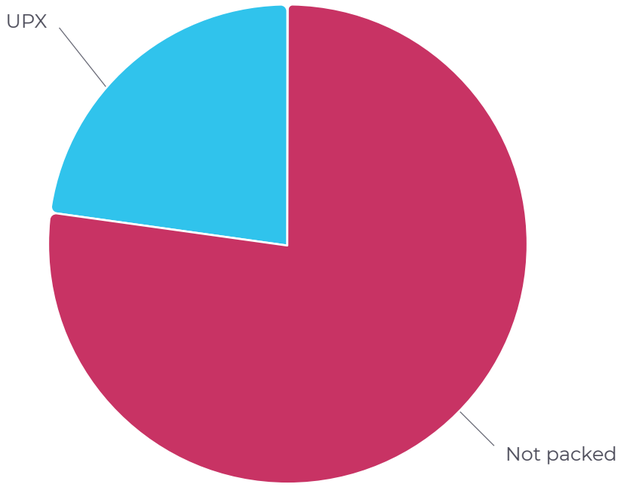


Figure 7: Top packers used to protect executable malware payloads, January-June 2023.

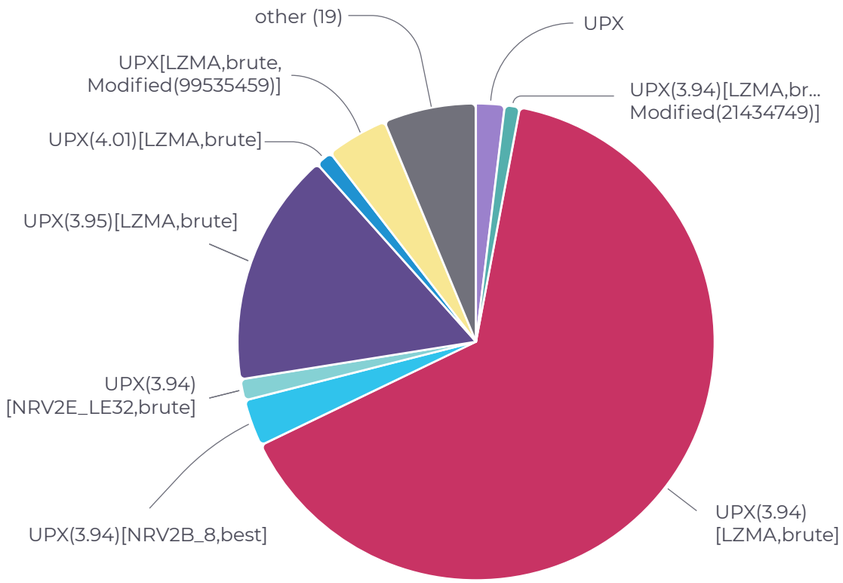


Figure 8: Top versions of packers used to protect executable malware payloads, January-June 2023.

6. Recommendations & Forecast

Threat actors continue to pursue the greatest ROI for their efforts in terms of financial gains or produced disruptions. Opportunistic attacks persist while tailored OT and IoT threat activity is a distinct risk for owners and operators of processes that tolerate little-to-no downtime. In a world where increased technology dependence is met with inherent risks, increased levels of automation and the adoption of machine learning and artificial intelligence capabilities have captured the attention of cyber defenders as well as adversaries.

While security by design is another hot button security topic today, it won't solve for existing vulnerabilities in deployed technologies.

Targeted attacks will tailor exploitation to a specific, well-researched victim organization, location, or both. Threat actors will continue to pursue living off the land techniques to evade security and extend their reconnaissance efforts to increase the severity of potential exploitation, disruption, and/or damage. Finally, accidental impacts – human error or attacks slipping out of scope to impact OT and IoT – though not always publicly reported, are still fairly common and will become more costly as interoperability continues to drive organizational missions and business decisions.

As listed in the many vulnerabilities reported and catalogued by CISA and NIST, there continue to be thousands of known vulnerabilities in OT/ICS machines and devices and threat actors are more aggressively probing Enterprise/IT, OT, and IoT networks across the globe. At the same time, threat actors are growing in capacity and sophistication of capabilities and enhanced TTPs. They continue to look for new access points – in networked communications, hardware, software, supply chain intrusions, and vendor access and management and more. Despite a limited number of attacks originating in OT networks, the potential for attacks to find their way to OT assets via Enterprise/IT and IoT connectivity remains foreboding and plausible. Even when IT attacks don't cross into OT systems, too often OT networks and processes are hampered by attacks on the IT systems they've come to rely upon.

The risks of loss of view and loss of control scenarios for critical infrastructure that underpins our health and wellness, economy and national security, are urgent and require attention. Many practical recommendations can mitigate these risks and ultimately limit the severity of threat actor campaigns and impacts. Vulnerability management, hardening systems, limiting privileged access, practicing proper network segmentation, isolating and testing transient devices, logging events for security analysis, limiting remote access, and planning for robust incident response and operational resilience involving stakeholders at every level of an organization are continued recommendations to prevent worst-case cybersecurity scenarios.

Nozomi Networks Labs is dedicated to continuously tracking the evolving threat landscape of industrial and critical infrastructure security.

Our awareness and visibility across the globe enable us to assess the growing number of CVEs, analyze the most persistent threats based on alerts detected by our products deployed in the field, and build more relevant context into our products. We continue to select, enumerate and test OEM vendor technologies, embedded components, manufactured IoT devices, metering and sensing technologies, web interface access points, and more. We invite you to review our latest **Nozomi Networks Labs blogs** from the first half of 2023, focused on device flaws and firmware vulnerabilities across real-time locating systems, in electronic devices, automation controllers, drones and more.

7. References

[1] Sergiu Gatlan, **"Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day,"** BleepingComputer, February 10, 2023.

[2] Ravie Lakshmanan, **"New Mirai Botnet Variant 'V3G4' Exploiting 13 Flaws to Target Linux and IoT Devices,"** The Hacker News, February 17, 2023.

[3] Jessica Davis, **"Killnet DDoS attacks inflicting damage on healthcare: 'This is war',"** SC Magazine, February 13, 2023.

[4] Carrie Pallardy, **"Looking at the Dole Cyberattack and the Future of Critical Infrastructure Cybersecurity,"** InformationWeek, March 3, 2023.

[5] **"The criminal use of ChatGPT - a cautionary tale about large language models,"** Europol, March 27, 2023.

[6] Eduard Kovacs, **"Irrigation Systems in Israel Disrupted by Hacker Attacks on ICS,"** SecurityWeek, April 13, 2023.

[7] Bekah Morr, **"Dallas is still under a ransomware attack. Here's what's impacted,"** Kera News, June 1, 2023.

[8] Ken Proska, Daniel Kapellmann Zafra, et al. **"COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises,"** Mandiant, May 25, 2023.

[9] Lawrence Abrams, **"New MOVEit Transfer zero-day mass-exploited in data theft attacks,"** BleepingComputer, June 1, 2023.

[10] Ravie Lakshmanan, **"New PowerDrop Malware Targeting U.S. Aerospace Industry,"** The Hacker News, June 7, 2023.

[11] **"Swiss websites hit by DDoS attack ahead of Zelenskiy video address,"** Reuters, June 12, 2023.

[12] Stephen Cauffman, **"CISA Releases White Paper Highlighting R&D Needs and Strategic Actions for Enhancing the Resilience of Critical Infrastructure,"** Cybersecurity & Infrastructure Security Agency, May 10, 2023.

[13] Caitlin Condon, **"Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability,"** Rapid7, June 1, 2023.

[14] @FalconFeedsio, **"Clop #ransomware group,"** Twitter, June 16, 2023.

[15] **"CISA and Partners Release Joint Advisory on Understanding Ransomware Threat Actors: LockBit,"** Cybersecurity & Infrastructure Security Agency, June 14, 2023.

[16] **"Understanding Ransomware Threat Actors: LockBit: Alert Code AA23-1651,"** Cybersecurity & Infrastructure Security Agency, June 14, 2023.

[17] **"FBI Flash: CU-000167-MW,"** Federal Bureau of Investigation, April 19, 2022.

[18] Check Point Research Team, **"Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks,"** Check Point, January 5, 2023.

[19] Ben Herzberg, **"3 healthcare data vulnerabilities to be mindful of in 2023,"** SecurityMagazine, January 18, 2023.

[20] Moreno Carullo, **"ChatGPT-4: AI's Evolving Capabilities and Consequences for Cybersecurity,"** Nozomi Networks, March 14, 2023.

[21] **"Pause Giant AI Experiments: An Open Letter,"** Future of Life Institute, March 22, 2023.

[22] David Nield, **"How ChatGPT—and Bots Like It—Can Spread Malware,"** WIRED, April 19, 2023.

[23] Vladislav Tushkanov, **"What does ChatGPT know about phishing?,"** SecureList, May 1, 2023.

[24] **"GitHub Copilot,"** Github.

[25] **"The criminal use of ChatGPT - a cautionary tale about large language models,"** Europol, March 27, 2023.

[26] **"Cybersecurity Alerts & Advisories,"** Cybersecurity & Infrastructure Security Agency.

[27] Nozomi Networks, **"upx-recovery-tool,"** Github, December 12, 2022.

[28] Ravie Lakshmanan, **"Chinese Hackers Using Never-Before-Seen Tactics for Critical Infrastructure Attacks,"** The Hacker News, June 26, 2023.

NOZOMI NETWORKS

Cybersecurity for OT 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.

nozominetworks.com

NN-SEC-RP-FULL-2023-IH-001