NOZOMI NETWORKS LABS

RESEARCH REPORT

OT/IoT Security Report

A Deep Look Into the ICS Threat Landscape

2022 2H Review | January 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 4

2. The Threat Landscape 6
   - 2.1 Hacktivists Launch Disruptive Cyberattacks 7
   - 2.2 Healthcare Hacks and Attacks 9

3. Attack Statistics From the ICS Field 10
   - 3.1 Types of Intrusion Alerts 11
   - 3.2 Most Commonly Detected Malware Categories 12

4. The IoT Botnet Landscape 13
   - 4.1 Protocols Involving Hard Coded Credentials 14
   - 4.2 Attack Source Locations 15
   - 4.3 Top Credentials Used 16
   - 4.4 Top Number of Unique Attacker IPs 17
   - 4.5 Top Attacker IP Addresses 18
   - 4.6 Top Executed Commands 19

5. The Vulnerability Landscape 20
   - 5.1 Analysis of ICS-CERT Advisories 21

6. Recommendations & Forecast 23
   - 6.1 Expert Recommendations and 2023 Forecast 24

7. References 26

How to Read This Report - This report is ideally read on a device. To navigate back and forth through the report, use the links in the Table of Contents, the links on section divider pages, or header links.

1. Introduction

The cyber threat landscape is constantly in flux, with new threats emerging and old ones evolving.

As technology advances, so do the methods that malicious actors use to gain access to sensitive information or launch disruptive attacks.

Cyberattacks focusing on IoT-connected devices present an additional challenge for critical infrastructure organizations in 2023, due to the large number of vulnerable smart devices that can be compromised remotely.

Attackers exploit weaknesses in device security or take advantage of misconfigured settings to gain control over vulnerable equipment—sometimes resulting in physical damage to underlying structures like buildings or energy grids—or to steal confidential data from connected systems.

During the first half of 2022, Russia's invasion of Ukraine had a significant impact on the threat landscape. We reported various threat actors at play in the cyberwarfare arena, the use of wiper malware, the emergence of ICS malware tailored to target specific OT protocols, and increasing interest in theft of technology source code by threat groups such as Lapsus$. Although the Russia/Ukraine war was at its peak earlier this year, remnants from the heightened conflict continued to trickle down into the rest of 2022.

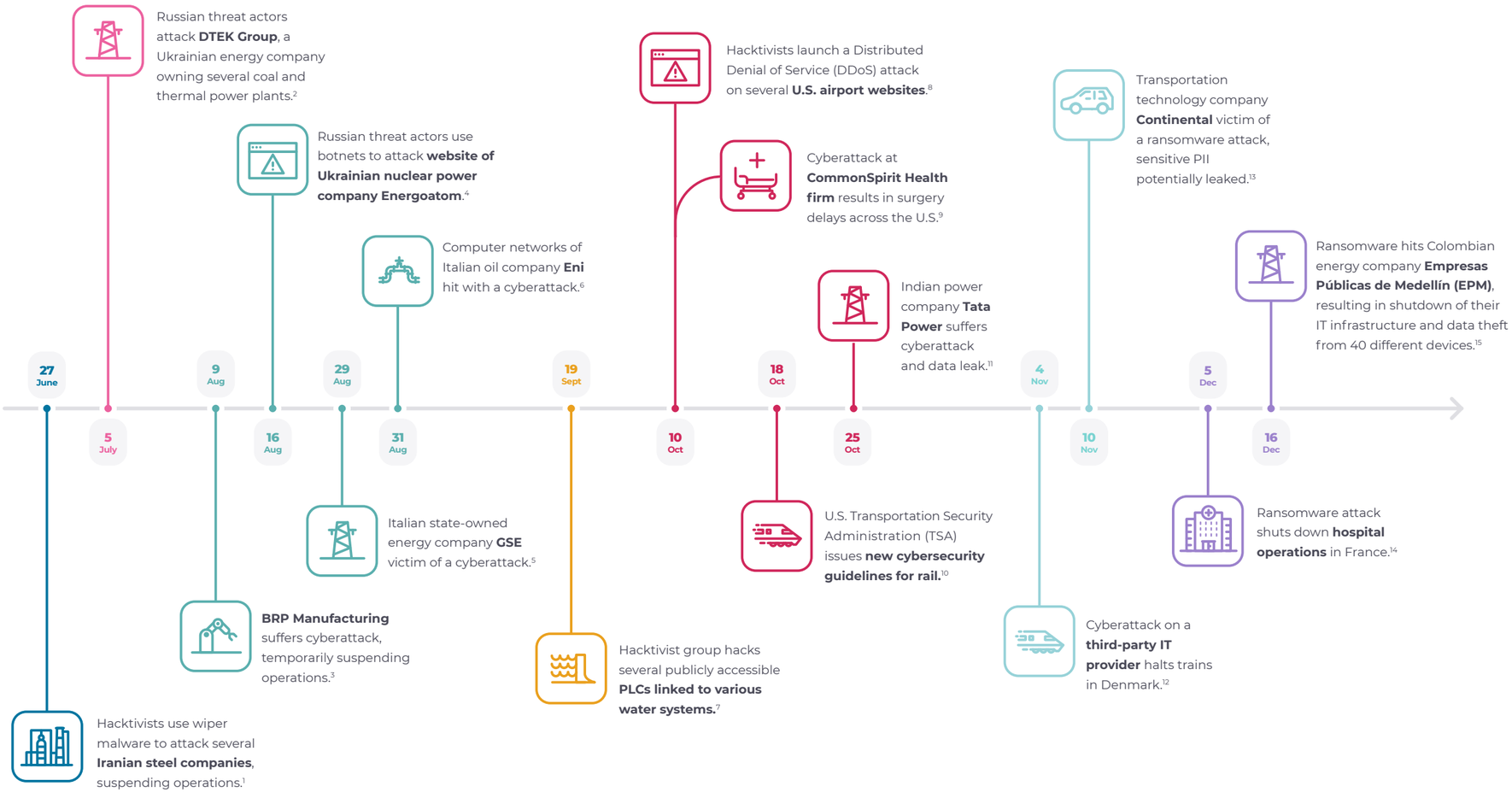
Over the past six months we have seen cyberattacks on critical infrastructure affecting industries ranging from transportation to healthcare. Continued attacks on railroads have prompted guidelines to help rail operators secure their assets. Hacktivists have opted to use wiper malware to launch disruptive attacks on critical infrastructure, to further their political stance in the Russia/Ukraine war. As cyber threats evolve and intensify, it is important to understand how threat actors are targeting the Operational Technology (OT) and Internet of Things (IoT) devices embedded in critical infrastructure.

In this report, Nozomi Networks Labs evaluates the threat landscape from July to December 2022 to report on notable cyberattacks on critical infrastructure, threat actor intrusion tactics, insights from our IoT honeypots, and analysis of ICS-CERT advisories to determine which industries are most vulnerable. We also provide recommendations for strengthening defenses and a forecast of emerging threats to help prepare for 2023.

Timeline of Notable Cyber Events in the Second Half of 2022

In the first half of 2022, we saw the impact of the Russia/Ukraine war on the cyber threat landscape.

In the second half of 2022, we've continued to see cyberattacks on critical infrastructure (namely rail), hacktivists causing disruptive attacks, thefts of technology source code, and use of wiper malware.



2 The Threat Landscape

2.1 Hacktivists Launch Disruptive Cyberattacks **7**

2.1.1 Rail Attacks on the Rise 8

2.1.2 U.S. Transportation Security Administration (TSA) Rail Directive 8

2.2 Healthcare Hacks and Attacks **9**

2.1 Hacktivists Launch Disruptive Cyberattacks

Three major steel companies in Iran – the Mobarakeh Steel Company (MSC), Khouzestan Steel Company (KSC) and Hormozgan Steel Company (HOSCO) – were hit by a cyberattack at the end of June continuing into July 2022.

These attacks, which caused website and production line disruptions, were claimed by a hacktivist group dubbed Gonjeshke Darandethat.[16] This group had previously taken responsibility for a cyberattack that deployed wiper malware on the Iranian train system earlier in the year.

This incident brings to light the vulnerability of critical infrastructure to malicious actors, regardless of their motives or affiliations.

Wiper malware is a type of malicious malware designed to erase or wipe out data and systems on a targeted computer or device. It differs from traditional ransomware in that it does not hold data for ransom but instead destroys it completely. Our 1H 2022 Security Report discusses the emergence of five new types of wiper malware on the market, and their effects on critical infrastructure.

These disruptive attacks serve as yet another reminder of the growing threat posed by hacktivists around the world. Such attacks can cause significant disruption and damage if not detected quickly enough; fortunately, there are steps businesses can take to protect themselves from similar incidents occurring in the future.

By investing in robust security measures, regular backups, and employee training programs, organizations can greatly reduce their risk of being targeted by hacktivists looking to wreak havoc with malicious software like wiper malware.

Hacktivists are shifting tactics from data theft and Distributed Denial of Service (DDoS) attacks to leveraging wiper malware to cause disruptive attacks on critical infrastructure.

2.1.1 Rail Attacks on the Rise

In November, Continental – an automotive and rail technology giant that develops cutting-edge technologies such as automated braking systems, vehicle monitoring systems, and navigations systems – was hit with a cyberattack.[17] The attackers had already breached Continental's networks before they struck, allowing them to gain access to numerous technical documents and source code pertaining to Continental's advanced technologies. Attackers accessing source code for these technologies is cause for major concern.

Attacks against rail systems have been growing in frequency, making this sector an attractive target to all threat actor types at play (i.e. nation-state, hacktivists, cybercriminals). Attackers may seek out private customer information like credit card numbers or personal data such as addresses or Social Security numbers for identity theft purposes. Additionally, they could attempt to sabotage operations by causing delays or disruption of services through DDoS attacks on websites or applications used within the network. By disrupting service schedules, attackers can cause significant financial losses for companies providing these services as well as create public safety hazards.

2.1.2 U.S. Transportation Security Administration (TSA) Rail Directive

The attack on Continental came after the U.S. Transportation Security Administration (TSA) issued cybersecurity requirements for rail and transit in October. TSA's new cybersecurity requirements revolve around four key areas: network segmentation, access control, monitoring/detection and patch management. This guidance is designed to strengthen the security of rail and transit systems by helping companies identify potential risks and vulnerabilities in their infrastructure.

2.2 Healthcare Hacks and Attacks

Healthcare facilities have become a prime target for cybercriminals due to the sensitive nature of their data.

Hospitals rely heavily on technology like medical records and imaging systems to provide patient care, so any disruption in service can cause significant harm to patients' health. As a result, hospitals may be more willing to pay ransoms than other organizations in order to regain access to their systems quickly. Additionally, healthcare providers often have access to medical records that contain financial information such as insurance numbers and credit card information.

Recent cyberattacks on hospitals during the second half of 2022 have given rise to new fears about healthcare systems being vulnerable to hackers. On October 10, 2022, a ransomware attack hit CommonSpirit Health, the fourth-largest U.S. health system with 140 affiliate hospitals. The attack led to delays in surgeries and other patient operations. There has also been a series of cyberattacks across Europe. In December, a ransomware attack at French hospital Corbeil-Essonnes resulted in a data leak and disruption of operations.

To reduce their vulnerability, many hospitals are developing comprehensive cybersecurity strategies that involve regularly monitoring networks for suspicious activity or implementing robust anti-virus software solutions. Additionally, many are investing in employee training so that staff members are aware of cyber threats and know how to respond if they become victims of an attack.

However, with limited resources and lack of cybersecurity expertise, it can also be difficult for hospitals to implement the latest security technology or hire additional personnel to help secure their systems.

3 Attack Statistics From the ICS Field

3.1 Types of Intrusion Alerts 11

3.2 Most Commonly Detected Malware Categories 12

3.1 Types of Intrusion Alerts

In this chapter, we share various statistics sourced from the fully anonymized detection telemetry of participating customer environments.

Threat actors can steal "clear text passwords" and guess "weak passwords" to gain unauthorized access into devices. Those alerts, coupled with “multiple access denied events” within a short time span, could indicate a potential brute force attack.

Other alerts like “TCP SYN flood”, where the threat actor floods a server with connection requests, could also indicate an attempted Denial of Service (DoS) attack.

Most Critical Types of Intrusion Alerts

July to December 2022

Cleartext password	**2,462,720**
Weak passwords	**1,666,146**
Packet rule match	**735,424**
Weak encryption	**511,138**
TCP SYN flood	**474,333**
Malformed network packet	**364,525**
Multiple Access Denied events	**359,263**
Malformed OT protocol packet	**242,000**
Invalid IP	**133,761**
Variable flow anomaly	**51,047**
Malicious domain	**41,609**
Unsupported function request	**35,127**
Multiple unsuccessful logins	**33,122**

Network scan	**28,526**
Suspicious activity	**11,753**
PUA detection	**10,419**
TCP flood	**9,916**
Anomalous packets	**5,618**
Bad reputation ip	**5,528**
Malware detection	**5,286**
OT protocol packet injection	**4,841**
MITM attack	**3,175**
UDP flood	**2,557**
Malformed TCP layer	**2,154**
Illegal parameters request	**1,984**
Brute force attack	**536**

3.2 Most Commonly Detected Malware Categories

There are many different categories of malware, and they vary in terms of what they do and how they are spread. Over the past six months, Trojans were the most common malware detected targeting enterprise networks, Remote Access Tools (RATs) targeted OT, and DDoS malware targeted IoT devices.

Most Commonly Detected Malware Categories

July to December 2022

Affected Environment	Malware	Number of Detections
IT	Trojan	**49,935**
OT	RAT	**3,392**
IT	Dualuse	**1,856**
IT	RAT	**523**
IT	Ransomware	**478**
IT	Loader	**156**
IT	Worm	**16**
IT	DDoS	**15**
IT	Hacktool	**6**
IT	Infostealer	**6**
IT	Phishing	**3**
IoT	DDoS	**2**
OT	DDoS	**2**
IT	Bootkit	**1**
OT	Infostealer	**1**

4 The IoT Botnet Landscape

4.1 Protocols Involving Hard Coded Credentials 14
4.2 Top Attacker Countries 15
4.3 Top Credentials Used 16
4.4 Top Number of Unique Attacker IPs 17
4.5 Top Attacker IP Addresses 18
4.6 Top Executed Commands 19

4.1 Protocols Involving Hard Coded Credentials

In this chapter we share unique data collected by Nozomi Networks Labs honeypots. These passive security systems are used to detect would-be attackers by simulating an asset which has value to the attacker. We also compare against trends from the first half of the year, available in our 2022 1H report. 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.

The SSH protocol was designed as a secure alternative to Telnet; both SSH and Telnet allow users to make changes, configure settings, and manage remote systems. Despite the security benefits of SSH, the majority of organizations continue to use the outdated Telnet in their networks today. This exposes them to attacks by threat actors who actively target devices with Telnet implementations that are unpatched or missing a VPN or firewall configuration.

Figure 1 shows that Telnet is currently being targeted more than SSH, with Telnet at 70% and SSH at 30%.

We will likely see targeting between Telnet and SSH fluctuate, depending on the most prevalent botnet types over a certain period, their distribution, and the protocols they support.

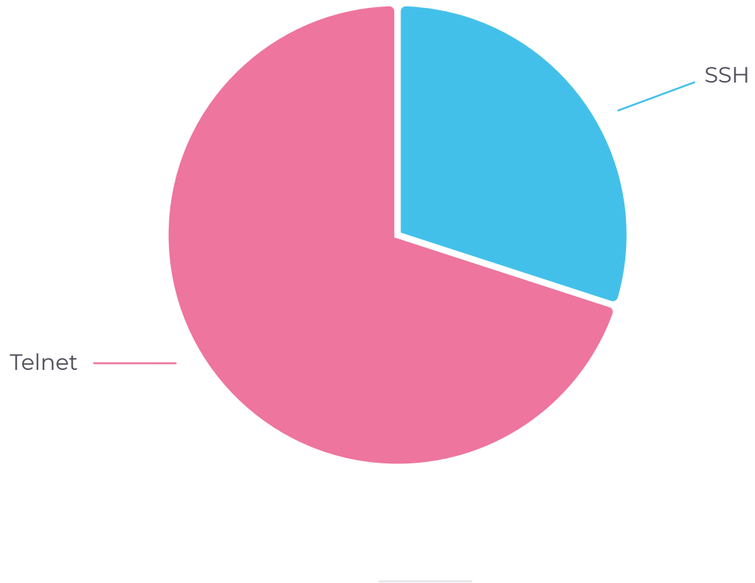


Figure 1: Protocols involving hard coded credentials, July-December 2022.

4.2 Attack Source Locations

Modern technology has created a challenging attribution problem for cyber defenders. It can be difficult to determine which devices are being controlled by an attacker because they are often routed through different countries and can be hosted on multiple servers within a given network.

Figure 2 shows that over the last six months, devices in the United States, China, and South Korea were leveraged by threat actors to initiate attacks more than devices in other countries.

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.

When we compare the first half and the second half of 2022, we see very similar attacker countries. However:

UK was previously a top attacker country in the first half of 2022. It has been replaced by Japan in the second half of 2022.

Additionally:

South Korea and Taiwan are on the rise, which could be due to increased device connectivity in the region.

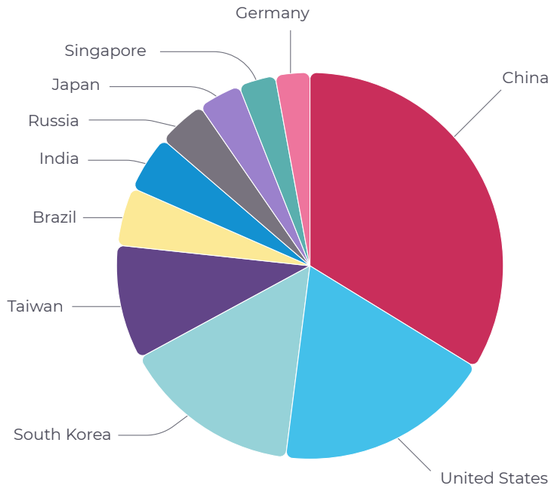


Figure 2: Top countries where compromised devices are used to execute attacks July-December 2022.

4.3 Top Credentials Used

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.

Our research found the same set of credentials being used to access different systems, but with 2x or 3x frequency compared to earlier in 2022.

This increase in botnet activity could be related to botnets using default credentials in attempts to gain access.

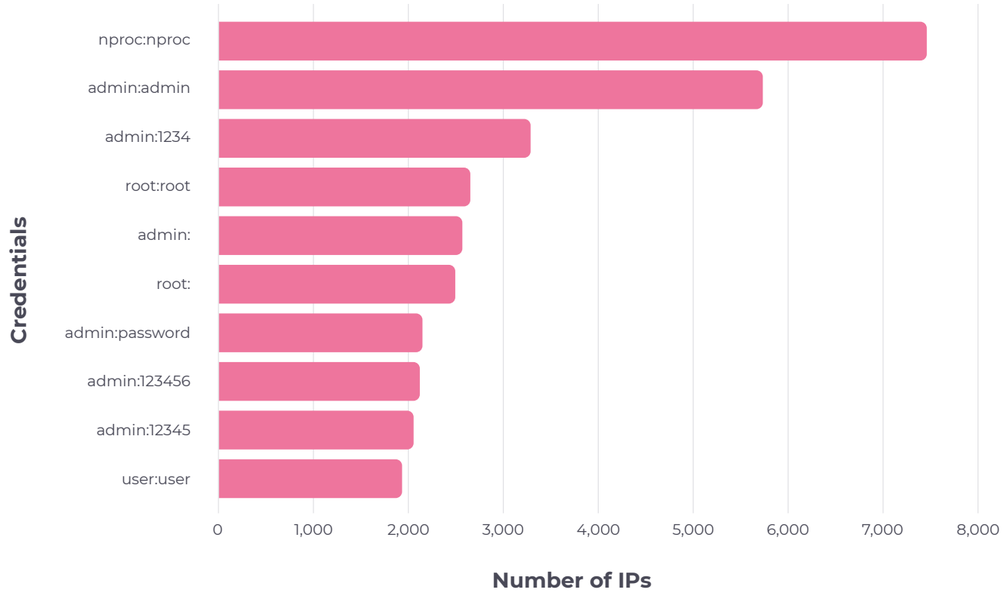


Figure 3: Top credentials used July-December 2022.

4.4 Top Number of Unique Attacker IPs

We define “unique” as non-repetitive Indicators of Compromise (IoCs) collected by Nozomi Networks Labs honeypots within each day.

Figure 4 shows the number of unique attacker IPs that have targeted our publicly facing IoT honeypots between July and December 2022.

This graph represents botnets, either compromised or attacker owned devices, that are attempting to infect our honeypots.

This showcases that threat actors are expanding the size of their botnets to cause more harm and maximize their profits.

We saw significant spikes during the months of July, October, and December. These numbers fluctuate based the amount of devices being infected vs. remediated on a daily basis.

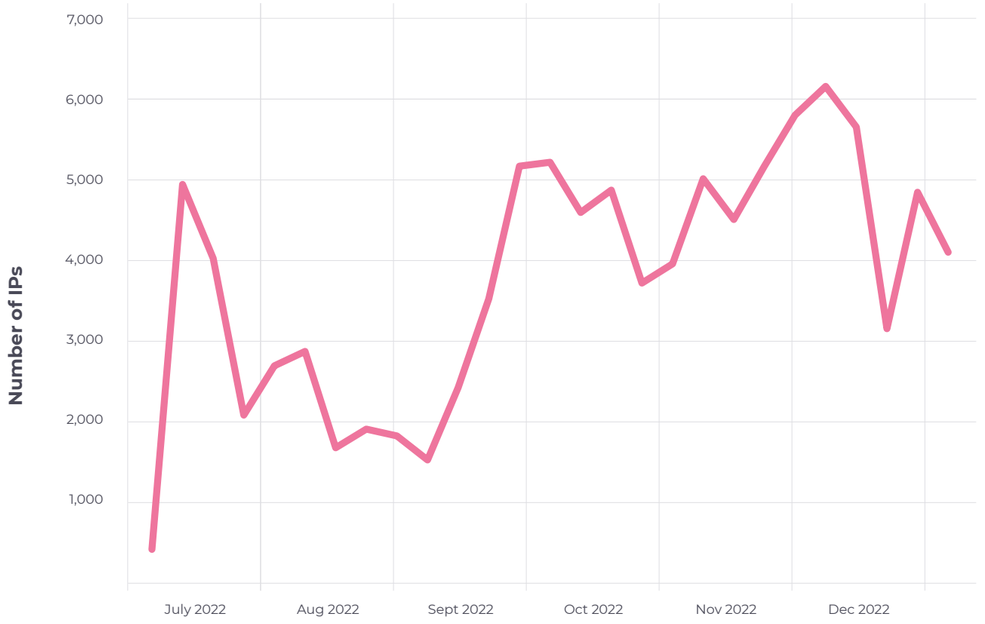


Figure 4: Unique attacker IPs July-December 2022.

4.5 Top Attacker IP Addresses

Here are malicious IP addresses attempting to access our IoT honeypots, with the top entry associated with over 70,000 attempts. This is a significant increase from the first six months of the year, where the top attacker IP made only 30,000 attempts.

We also observed that some IPs were used repeatedly. Repetitive IPs indicate that threat actors were able to maintain persistence in compromised devices for a long period of time, mostly due to weak credential and patch management.

By reusing the same IP addresses which previously belonged to legitimate organizations, threat actors can disguise their malicious activity by making it appear to be coming from a trusted source which could throw off Intrusion Detection Systems (IDS). This also represents attackers maintaining consistent access to vulnerable systems, allowing them to establish long-term campaigns or operations.

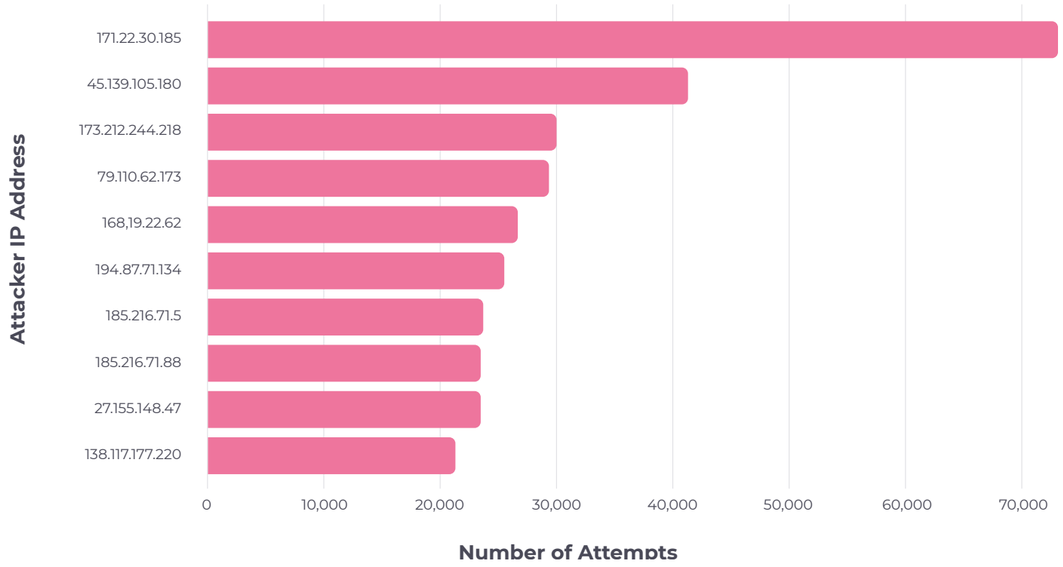


Figure 5: Top attacker IPs July-December 2022

4.6 Top Executed Commands

Following initial access, threat actors execute commands on a system that will allow them to maintain persistence and escalate privileges.

Figure 6 shows the top executed commands from July through December 2022.

1. enable **3. sh**

2. shell **4. system**

These top 4 executed commands are **more prevalent** in comparison to the other commands and **found in the scripts of multiple malware families**.

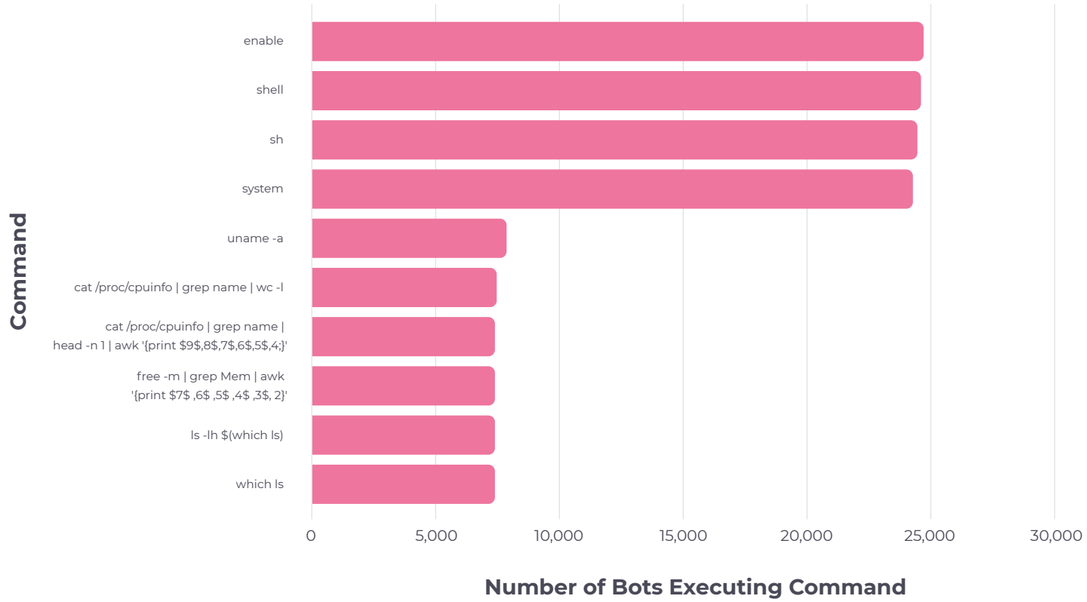


Figure 6: Top executed commands July-December 2022.

5 The Vulnerability Landscape

5.1 Analysis of ICS-CERT Advisories **21**

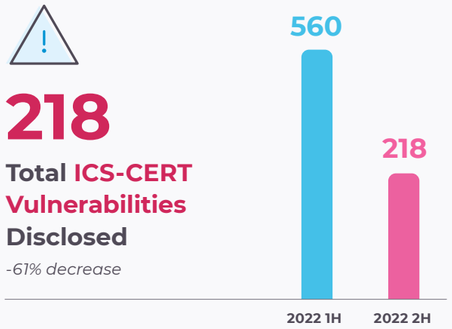
5.1.1 Number of CVEs Released in 2022 by Sector 21

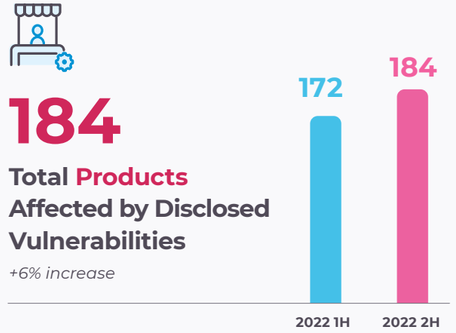
5.1.2 Number of CWEs Associated with CVEs, July-December 2022 22

5.1 Analysis of ICS-CERT Advisories

In this section we analyze ICS-CERT advisories, published by CISA, from the second half of 2022. From July–December 2022, there were 218 Common Vulnerabilities and Exposures (CVEs) released.

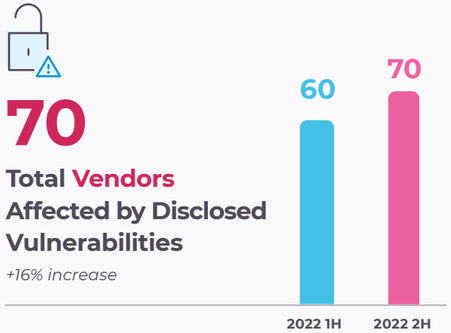
There were 70 affected vendors mentioned in these advisories, with 184 associated products. CVE reporting was down by 61% compared to the first half of 2022, while mentioned vendors went up 16% and affected products were up 6% from the first half of 2022.

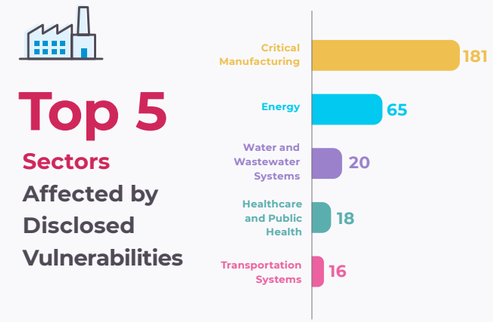




5.1.1 Number of CVEs Released in 2022 by Sector

Critical manufacturing continues to be the most vulnerable sector, based on disclosed ICS-CERT vulnerabilities affecting products used in that industry. Energy remains the second industry most affected by vulnerabilities. Healthcare is still in the top five, however, two new vulnerable industries have emerged: Water & Wastewater and Transportation Systems. This is reflective of the various cyberattacks we have reported on water treatment facilities and rail/transit systems this year.



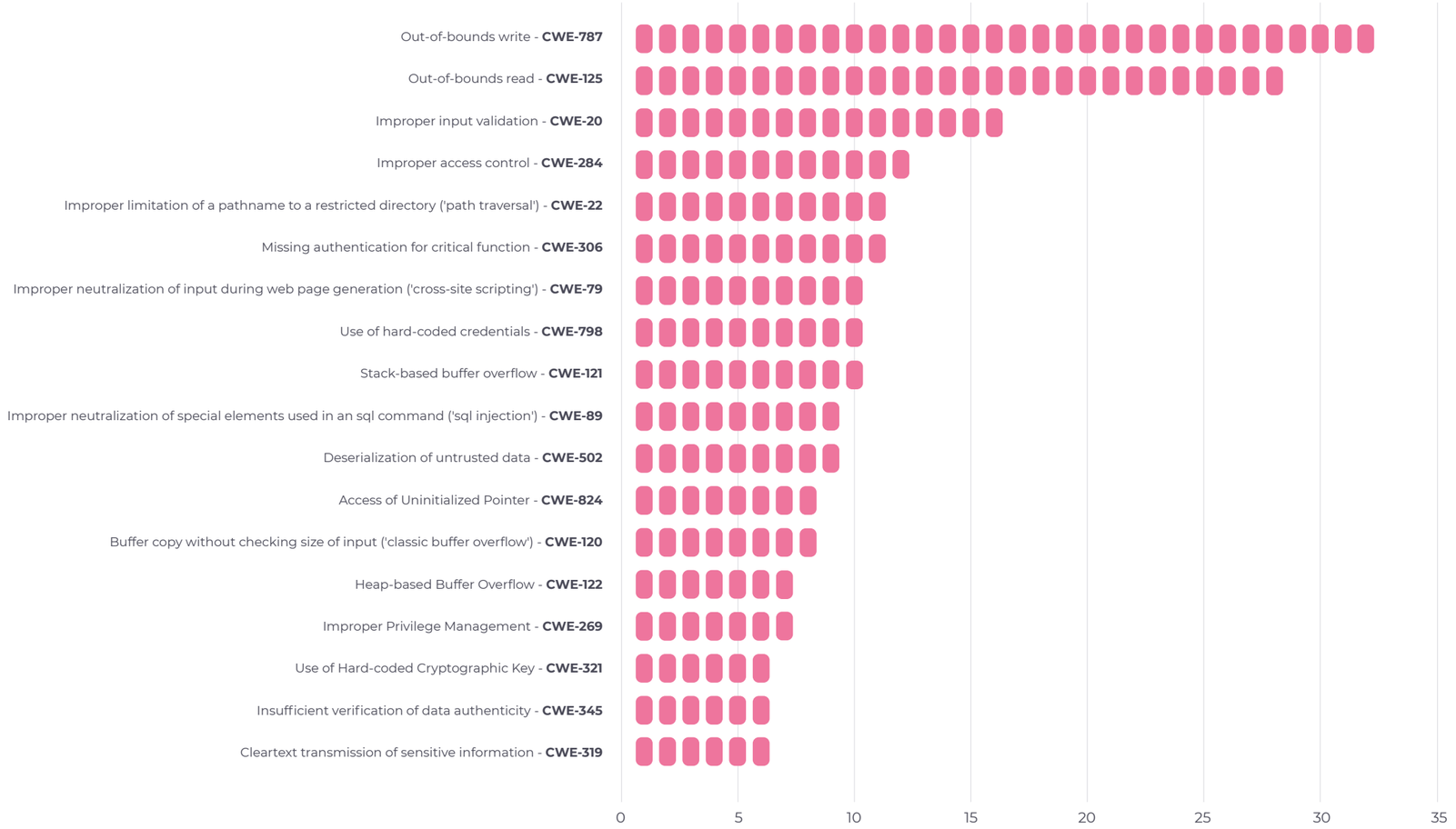


5.1.2 Number of CWEs Associated with CVEs, July-December 2022

This graph illustrates the top Common Weakness Enumerations (CWEs) associated with CVEs released in the second half of 2022. Out-of-Bounds Write (CWE – 787) and Out-of-Bounds Read (CWE – 125) increased significantly compared to the first half of the year, climbing to the top of the list. CWE-787 is a type of software vulnerability that is caused by a program writing to an area of memory outside its bounds, which could lead to code execution, or a crash. Respectively, CWE 125 is a software error that occurs when a program tries to read data from memory beyond the end of an array. These types of flaws can be exploited by attackers.

Other most reported critical weaknesses include improper input validation, improper access control, and use of hard coded credentials.

Understanding these common software and hardware security flaws can give organizations insights into how to better secure their networks.



6 Recommendations & Forecast

6.1 Expert Recommendations and 2023 Forecast **24**

6.1.1 Hybrid threat tactics 24

6.1.2 Quantum threats and preparation 24

6.1.3 Medical device exploits 25

6.1.4 Cyber insurance inflection point 25

6.1.5 AI-driven chatbots used for malicious purposes 25

6.1.6 Cybersecurity professionals will need to learn new skillsets 25

6.1 Expert Recommendations and 2023 Forecast

From what we observed in 2022, we expect the 2023 cyber threat landscape to be marked with continued complexity and sophistication as attackers evolve their strategies for exploiting vulnerable systems and networks.

Critical infrastructure organizations should prioritize proactive defense strategies to include network segmentation, asset discovery, vulnerability management, patching, logging, endpoint detection, and threat intelligence to protect against potential threats. Organizations should proactively safeguard their systems now, so they can be in a better position to combat cyberthreats that may arise in 2023.

Because cybersecurity is a complex and ever-evolving industry, it can be difficult to predict the next trends. However, we can make some educated guesses based on what we know now. The following are some of the key cybersecurity trends we expect to see in 2023:

6.1.1 Hybrid threat tactics

The lines that once categorized different types of threat actors are now blurred, which could lead to significant changes in the threat actor landscape. For example, the recent Continental ransomware attack was launched by hacktivists who used nation-state tactics to cause a physical disruption on railroads. Meanwhile, nation-state threat actors have been leveraging cyber-criminal tactics, such as ransomware, to cause disruption in critical environments. It will become increasingly difficult to categorize threat groups based on TTPs and motives, which have aided in attribution efforts in the past.

6.1.2 Quantum threats and preparation

As threat actors use the “store now, decrypt later” (SNDL) technique in preparation for quantum decryption, governments are taking steps to prepare against this future threat. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) released its **post-quantum cryptography initiative** on July 6, 2022, to prepare and safeguard critical infrastructure companies during this transition. As CISA rolls out this guidance, more companies will shift their focus to safeguarding their data now to reduce the risks of quantum decryption later.

6.1.3 Medical device exploits

Many medical devices are susceptible to cyberattacks due to the fact that the legacy systems they are using are no longer being manufactured and/or the software no longer supported. Threat actors use scanners and other types of tools to identify and exploit vulnerabilities in these devices and perform manipulative tactics or even launch cyberattacks. Apart from using scanners to exploit vulnerabilities, threat actors can access medical systems used to aggregate device data for broader analysis and monitoring. This manipulation could lead to malfunctions, misreadings, or even overdoses in automatic release of medication.

6.1.4 Cyber insurance inflection point

Cyber insurance is an important part of a comprehensive cybersecurity strategy. However, cyber criminals are conducting reconnaissance on cyber insurance claims policies and tailoring their ransom requests to match the amount of a cyber insurance payout. This could either cause premiums to significantly increase, or even dry out cyber insurance resources making it more difficult to file serious claims and receive payouts. Cyber insurance is not a cure for cyberattacks, in fact it could motivate cyber criminals. Companies should invest in cyber prevention, protection, and remediation as a first line of defense.

6.1.5 AI-driven chatbots used for malicious purposes

ChatGPT is a variant of the Generative Pre-trained Transformer (GPT) language model that is specifically designed to generate human-like text based on a given prompt. While ChatGPT can be used in a variety of applications, such as generating chatbot responses or creating content for social media, it can also be used in social engineering and phishing attacks. For example, a hacker could use ChatGPT to generate a phishing email that appears to be from a legitimate company or individual, complete with personalized greetings and specific details about the recipient. As these systems become more sophisticated, malicious threat actors could use them to write malicious code or develop exploits for vulnerabilities. This could reduce the time it takes to develop targeted threat campaigns, thus increasing the frequency of cyberattacks.

6.1.6 Cybersecurity professionals will need to learn new skillsets

As the threat landscape changes, organizations will need highly-skilled cyber professionals and more advanced cybersecurity solutions to defend against an increasingly sophisticated range of attacks. Cybersecurity professionals need to be able to adapt quickly as new threats emerge and to find new ways to defend their environments.

7. References

[1] 1.AJ Vicens, **"Iranian Steel Facilities Suffer Apparent Cyberattacks,"** Cyberscoop, June 27, 2022.

[2] Sean Lyngaas, **"Russian Hackers Allegedly Target Ukraine's Biggest Private Energy Firm,"** CNN, July 5, 2022.

[3] **"BRP Reports Cyberattack,"** BRP, August 9, 2022.

[4] **"Ukraine Nuclear Power Company Says Russia Attacked Website,"** Al Jazeera, August 16, 2022.

[5] Supantha Mukherjee and Elvira Pollina, **"Ransomware Group BlackCat Behind Italy's GSE Hacking, Researchers Say,"** Reuters, September 2, 2022.

[6] Daniele Lepido and Alberto Brambilla, **"Hackers Hit Italian Oil Giant Eni's Computer Network,"** Bloomberg, August 31, 2022.

[7] **"Cyberattackers Make Waves in Hotel Swimming Pool Controls,"** Dark Reading, September 19, 2022.

[8] Gloria Oladipo, **"Cyberattacks Force Over a Dozen US Airport Websites Offline,"** The Guardian, October 10, 2022.

[9] Cara Murez, **"Patient Care Delayed at Large Hospital Chain After Ransomware Attack,"** U.S. News, October 10, 2022.

[10] **"TSA Issues New Cybersecurity Requirements for Passenger and Freight Railroad Carriers,"** U.S. Transportation Security Administration, October 18, 2022.

[11] Ax Sharma, **"Hive Claims Ransomware Attack on Tata Power, Begins Leaking Data,"** BleepingComputer, October 25, 2022.

[12] Eduard Kovacs, **"Cyberattack Causes Trains to Stop in Denmark,"** SecurityWeek, November 4, 2022.

[13] Eduard Kovacs, **"Ransomware Gang Offers to Sell Files Stolen From Continental for $50 Million,"** SecurityWeek, November 10, 2022.

[14] **"Cyberattack Shuts Down French Hospital,"** Dark Reading, December 5, 2022.

[15] Lawrence Abrams, **"Columbian Energy Supplier EPM Hit by BlackCat Ransomware Group,"** BleepingComputer, December 16, 2022.

[16] Mihir Bagwe, **"Iranian Steelmaker Halts Production Following Cyberattack,"** Bank Info Security, June 27, 2022.

[17] Eduard Kovacs, **"Ransomware Gang Offers to Sell Files Stolen From Continental for $50 Million,"** SecurityWeek, November 10, 2022.

Cybersecurity and Analytics for All Your Connected Devices

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

nozominetworks.com