NOZOMI NETWORKS

Executive Summary

OT/IoT Security Report

A Deep Look Into the ICS Threat Landscape

2022 2H Review | January 2023

Executive Summary

The ever-evolving cyber threat landscape is undergoing constant changes as new malicious actors and tactics emerge.

As technology advances, cyber threat actors are using increasingly advanced methods to gain access to confidential information or launch disruptive cyberattacks. With the emergence of the Internet of Things (IoT), criminals have access to a plethora of connected devices and are now able to penetrate networks with multiple points of entry.

Over the past six months, cyberattacks have increased significantly, causing major disruption to industries ranging from transportation to healthcare. Railways, in particular, have been subject to attacks, leading to the implementation of measures designed to protect rail operators and their assets.

Additionally, hacktivists have employed wiper malware in an attempt to destabilize critical infrastructure to further their political stance in the Russia/Ukraine war.

As cyber threats evolve and intensify, it is important for organizations to understand how threat actors are targeting OT/IoT and the actions required to defend critical assets from threat actors.

In this report we cover:

- **Cyberattacks** on critical infrastructure over past 6 months
- **Hacktivists** leveraging malware to launch destructive attacks
- **Hospital systems** becoming increasingly targeted
- **Rail cyberattacks** and new protective guidelines
- **Intrusion alerts** affecting OT environments
- **Malware categories** affecting Enterprise, OT, and IoT
- **Recommendations** and 2023 **forecast**

2022 2H THREAT LANDSCAPE

July to December 2022

Exclusive insights from Nozomi Networks' IoT honeypots:

- **Protocols involving hard coded credentials**
- **Top attacker countries**
- **Top credentials used**
- **Unique attacker IPs**
- **Attacker IP addresses**
- **Top executed commands**

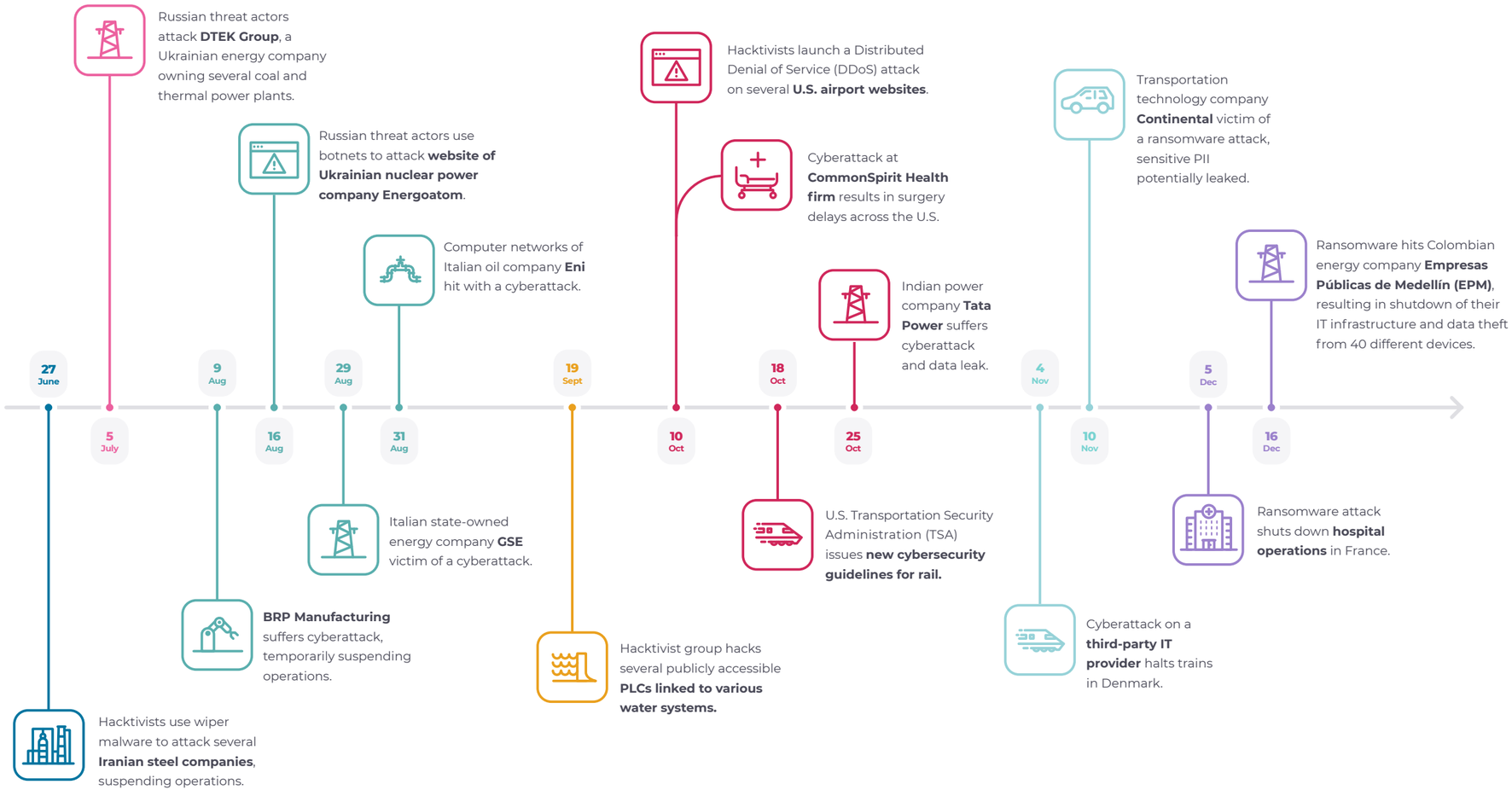
Timeline of Notable Cyber Events in the Second Half of 2022:

This timeline summarizes the most significant cyber events—cyberattacks, new policies, malware, etc.—from July to December 2022.

In the first half of the year, 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 disruptive cyberattacks on critical infrastructure sectors to include: rail, hospitals, manufacturing, and energy.

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.



In this report, 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. In the second half of 2022, we captured the following:

- **Protocols involving hard coded credentials:** Telnet is currently being targeted more than SSH, with Telnet at 70% and SSH at 30%.
- **Attack source locations:** Devices in the United States, China, and South Korea are leveraged by attackers to initiate attacks more than devices in other countries.
- **Top credentials used:** Default credentials continue to be used, but with double or triple frequency; indicating the presence of additional botnets attempting to gain access.
- **Top number of unique attacker IP addresses:** There were significant spikes in the number of unique IPs targeting OT/IoT in July, October, and November.
- **Top attacker IP addresses:** Malicious IP addresses attempted to access our IoT honeypots, with the top entry associated with over 60,000 access attempts, which has doubled since our last report.

TOP 4 EXECUTED COMMANDS

1. enable
2. shell
3. sh
4. system

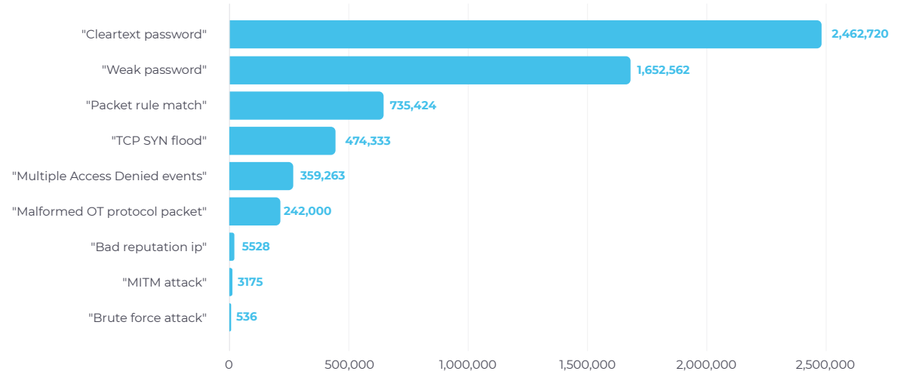
These commands are **more prevalent** in comparison to the other commands and **found in the scripts of multiple malware families**.

Attack Statistics From the ICS Field

July to December 2022

Most Critical Types of Intrusion Alerts

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.



See the full report for a complete data.

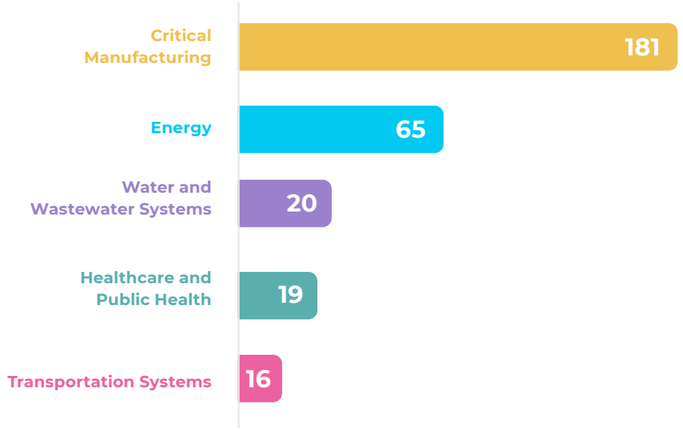
Most Commonly Detected Malware Categories

In the past 6 months, **Trojans** were the most common malware detected targeting enterprise networks, **Remote Access Tools (RATs)** targeted OT, and **DDoS malware** targeted IoT devices.

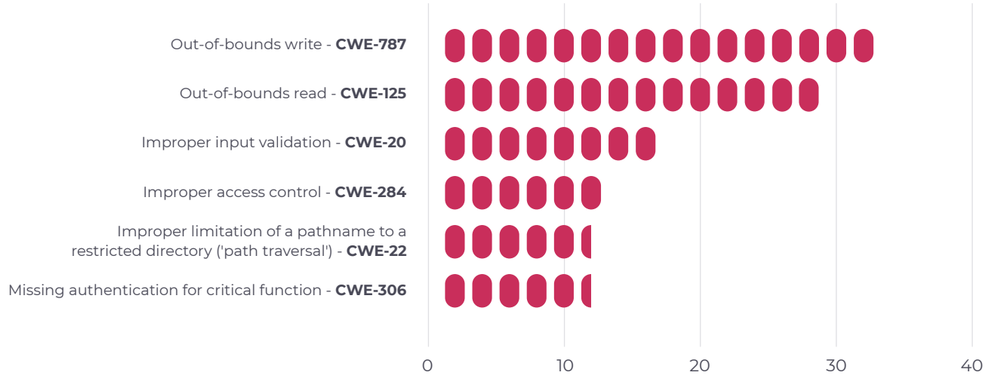
The Vulnerability Landscape

We analyzed ICS-CERT advisories, published by CISA, from July to December 2022.

Top 5 Sectors Affected by Disclosed Vulnerabilities



This graph illustrates the top Common Weakness Enumerations (CWEs) associated with CVEs released in the second half of 2022.



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.

Out-of-Bounds Write (CWE – 787) and Out-of-Bounds Read (CWE – 125) increased significantly compared to the first half of the year. Understanding these common software and hardware security flaws can give organizations insights into how to better secure their networks.

Recommendations

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

To protect against potential threats, critical infrastructure organizations should prioritize proactive defense strategies to include:

- Network segmentation
- Asset discovery
- Vulnerability management
- Patching
- Logging
- Endpoint detection
- Threat intelligence

Organizations should proactively safeguard their systems now, so they can be in a better position to combat cyberthreats that may arise in 2023.

What To Expect in 2023?

1. Hybrid threat tactics

It will become increasingly difficult to categorize types of threat actors based on TTPs and motives, which have aided in attribution efforts in the past.

2. Quantum threats and preparation

As threat actors use the "store now, decrypt later" (SNDL) technique in preparation for quantum decryption, CISA rolls out guidance to help organizations safeguard their data now to reduce the risks of quantum decryption later.

3. Medical device exploits

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.

4. Cyber insurance inflection point

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.

5. AI-driven chatbots used for malicious purposes

As these systems become more sophisticated, malicious threat actors could use them to write malicious code or develop exploits for vulnerabilities. They can also be misused to generate more convincing and grammatically accurate phishing/social engineering texts. All this could reduce the time it takes to develop targeted threat campaigns, thus increasing the frequency of cyberattacks.

6. Cybersecurity professionals will need to learn new skillsets

Cybersecurity professionals will need to adapt quickly as new threats emerge and to find new ways to defend their environments.

Download the OT/IoT Security Report

Nozomi Networks Labs analyzes the current threat landscape and shares:

- Recent hacktivist attacks on critical infrastructure
- ICS/OT/IoT device vulnerability and exploitation trends
- Predictions for the 2023 cybersecurity landscape

Download

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