



OT/IOT SECURITY REPORT | EXECUTIVE SUMMARY

Unpacking the Threat Landscape With Unique Telemetry Insight

August 2023





Executive Summary

The first half of 2023 was full of OT/IoT cybersecurity events, many of which are a continuation of the trends we've seen in 2022.

Ransomware continues to plague businesses of all sizes and sectors across the globe, while healthcare, energy, and manufacturing continue to be targeted by nation states, criminal groups, and hackers alike.

Meanwhile, new trends are always emerging. Groups are now tinkering with the potential to combine autonomy, machine learning and natural language models into emerging technologies with both positive and malicious motivations.

While the trends analysis in this report does not seek to unpack any single threat actor or attack campaign, we holistically track many threat actors targeting Nozomi Networks' customer environments and globally distributed IoT honeypots.

There are three main categories of OT/IoT cyber incidents: **opportunistic**, **targeted**, and **accidental**. Over the past six months, opportunistic attacks remain the most prevalent and will continue to flood traffic via DDOS attempts, enumerate common weaknesses and vulnerabilities for initial access, and trial and error malware strains regardless of network domains and target systems.

The number of vulnerabilities discovered in OT and IoT devices remains high, with several considered critical and/or easily exploitable. Increased process automation across the globe 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, sensing capabilities, transient devices, additional networks and business integrations is also adding new attack vectors and expanding the traditional threat landscape by the day.

This report features trend analysis leveraging open-source data and collated publicly available information and resources, as well as independent and unique telemetry data from Nozomi Networks.

We begin by reviewing the current threat landscape, the continuing trends of ransomware, and emerging trends like the advent of ChatGPT as well as targeting of the healthcare sector. We then expand on statistical analysis of recent attack patterns from 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.

THIS REPORT FEATURES



Review of the current threat landscape



Ransomware trends



Emerging cybersecurity trends



Statistical analysis of recent attack patterns



Unique telemetry data from Nozomi Networks deployments



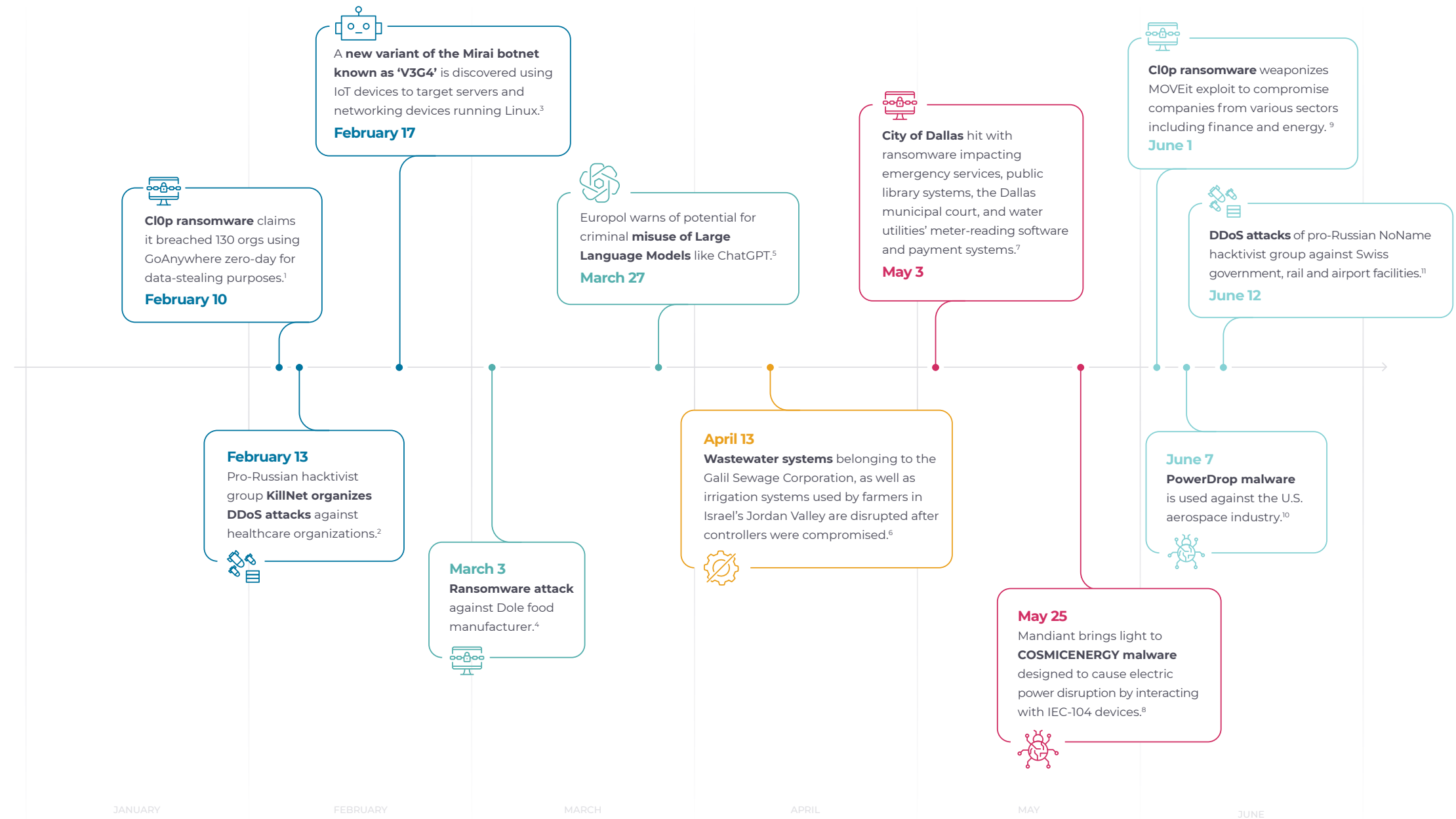
Timeline of Notable Cyber Events in the First Half of 2023

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.



Newly Discovered CVEs and Top CWEs

Between January 1 and June 15, 2023, CISA reported 171 new advisories detailing 641 vulnerabilities affecting various products from 62 different vendors.

When looking at CVEs impacting specific sectors, Critical Manufacturing is the most impacted, followed by Energy, Water, Food and Agriculture, and the Chemical sector.

Newly added CVEs impacting Food and Agriculture have increased significantly compared to the previous six months, bringing this industry into the top 5 affected by recently discovered and disclosed vulnerabilities.

For top Common Weakness Enumerations (CWEs) associated with CVEs released in the first half of 2023, Use-After-Free was surprisingly the most frequently discovered CWE during this reporting period. Historically this has been a less common CWE.

Out-of-Bound Read and Out-of-Bound Write operations remained in the top CWEs compared to the previous period.


STATS



171

new advisories reported by CISA



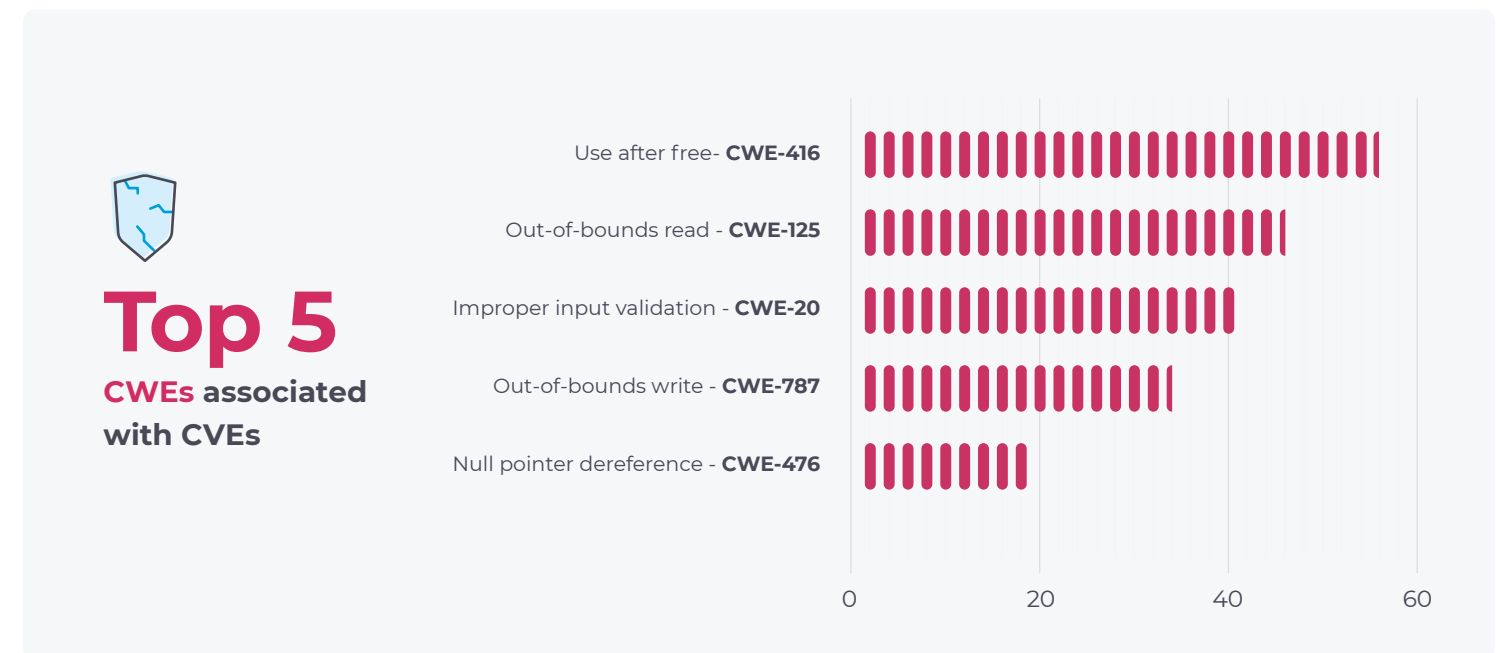
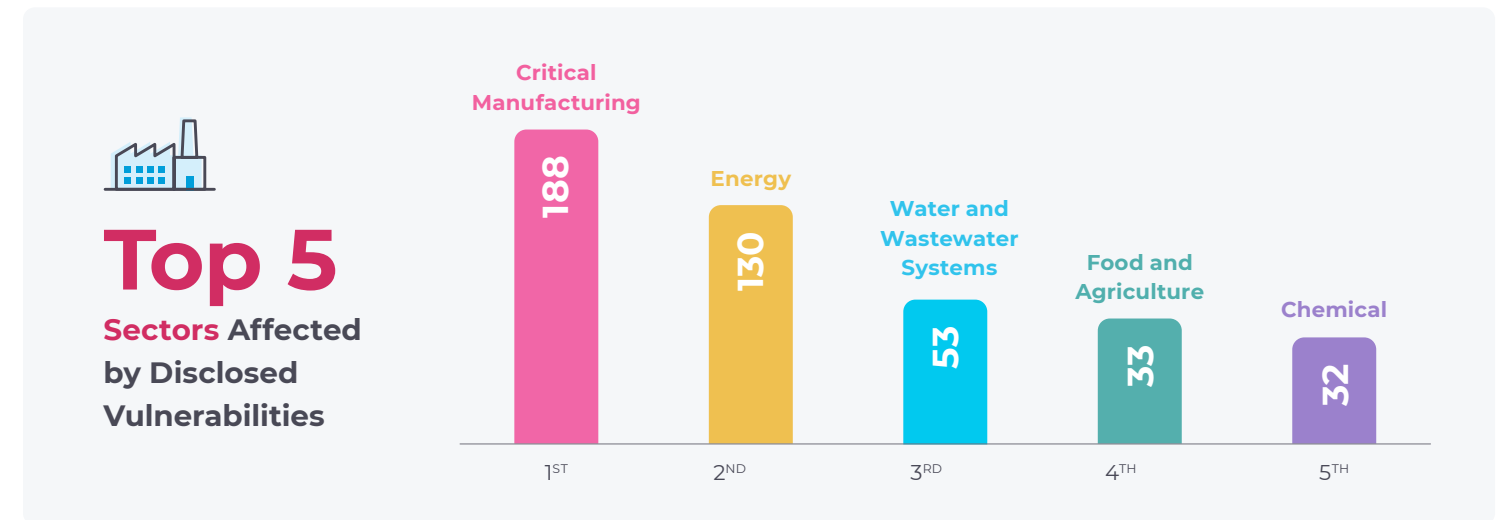
641

Total ICS-CERT Vulnerabilities Disclosed



62

Total Vendors Affected by Disclosed Vulnerabilities





Nozomi Networks Alerts

Our full report details total numbers of malware alerts by type, and breaks down alert types by network domain, industry, and a handful of regional country snapshots.

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.


“Trojan” and “Dualuse” are some of the most commonly detected alerts across Nozomi Networks’ customer base.

“Ransomware” remains a frequently recognized malware category across Enterprise/IT domains, causing significant damage to normal business operations all over the globe.


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 PREVALENT ALERT TYPES




Denial-of-Service (DOS)




Remote Access Trojan (RAT)




Trojan



Dualuse



Ransomware



Phishing

For intrusion alerts and possible threat hunting, here are the most frequent network activity detections across our customer networks:

Network Scan	27 %
Cleartext password	12 %
Weak password	8 %
Program transfer	7 %
Malformed traffic	6 %

The most triggered alerts vary depending on the industry. While Water Treatment facilities witnessed higher numbers of generic network scanning alerts typically associated with authorized scanning or threat actor probing, customers in Oil and Gas were more likely to experience alerts related to OT protocol packet injection.

OT protocol packet injection involves a correct protocol packet injected in the wrong context, such as a correct protocol message being sent in the wrong sequence. As a whole, many sectors share similar common alert types like poor credential management, cleartext password identification, and TCP flood alerts.

IoT Insights

In IoT network domains, **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.

Nozomi Networks’ distributed IoT honeypots witnessed between hundreds and thousands of unique attacker IP addresses daily. Some of the commands used after stealing credentials are generic and are commands 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.” Trusted keys are used to maintain persistent access, providing a way to connect via SSH to the compromised machine later.



How Are We Doing in 2023?

Good News for Defenders



More OT/ICS owners and operators have **invested in expanded visibility**, providing new telemetry data and greater understanding of threats.



Automation, **machine learning** and **artificial intelligence** have the potential to allow security teams to harness the power of data for operational resilience.

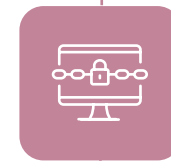


In the first half of this year, governments around the world have been working to **enhance cybersecurity legislation and critical infrastructure policy** at the national level.

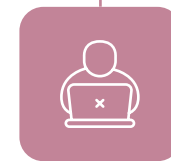
Threats to Watch For



The number of **vulnerabilities discovered in OT and IoT devices remains high**, with several considered critical and/or easily exploitable.



Healthcare, energy, and manufacturing continue to be **highly targeted sectors** by threat actors as **ransomware** continues to plague organizations.



Opportunistic attacks remain; **exploiting vulnerabilities, abusing credentials, and phishing** attempts for initial access, **DDoS** attempts, and **trojan** execution.

Download the OT/IoT Security Report

Nozomi Networks Labs analyzes the current
threat landscape and shares:

- Open-source trends analysis of attacks and vulnerabilities
- Threat landscape insights, ransomware and emerging technologies
- Statistical analysis of recent attack patterns from Nozomi Networks product deployments
- The IoT botnet landscape and attack patterns

[Download](#)



OT/IOT SECURITY REPORT

Unpacking the Threat Landscape With Unique Telemetry Insight

2023 1H Review | August 2023



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

© 2023 Nozomi Networks, Inc. | All Rights Reserved.