NOZOMI NETWORKS

Executive Summary

OT/IoT Security Report

Cyber War Insights, Threats and Trends, Recommendations

2022 1H Review | August 2022

Executive Summary

With the cyber threat landscape constantly changing, it is more important than ever to understand how it is impacting your organization. In the past six months, we have seen a surge in the frequency and complexity of attacks, as well as the use of new tactics by threat actors. Threats that were once considered unlikely have suddenly become commonplace.

For example, companies that were not previously targeted by ransomware are now finding themselves on the receiving end of these attacks. In addition to this shift, threat actors continue to obfuscate their malicious activity from detection by security solutions.

To strengthen security and minimize future threats, companies need real-time insight into their cyber risk exposure so they can make informed decisions about how best to protect themselves.

In this report we:

- **Review** the current state of cybersecurity.
- **Identify** key trends in the threat landscape, and offer solutions for addressing them.
- **Recap** the Russia/Ukraine crisis, highlighting new malicious tools and malware introduced, as well as how this conflict can give us insights into attacker capabilities.
- **Provide** insights into Internet of Things (IoT) botnets, corresponding Indicators of Compromise (IoCs), and threat actor Tactics Techniques and Procedures (TTPs).
- **Share** recommendations and forecasting analysis.

2022 1H THREAT LANDSCAPE

Since Russia began its invasion of Ukraine in February, we have seen:

Hacktivist activity

State-backed APTs and cyber criminals

Wiper malware

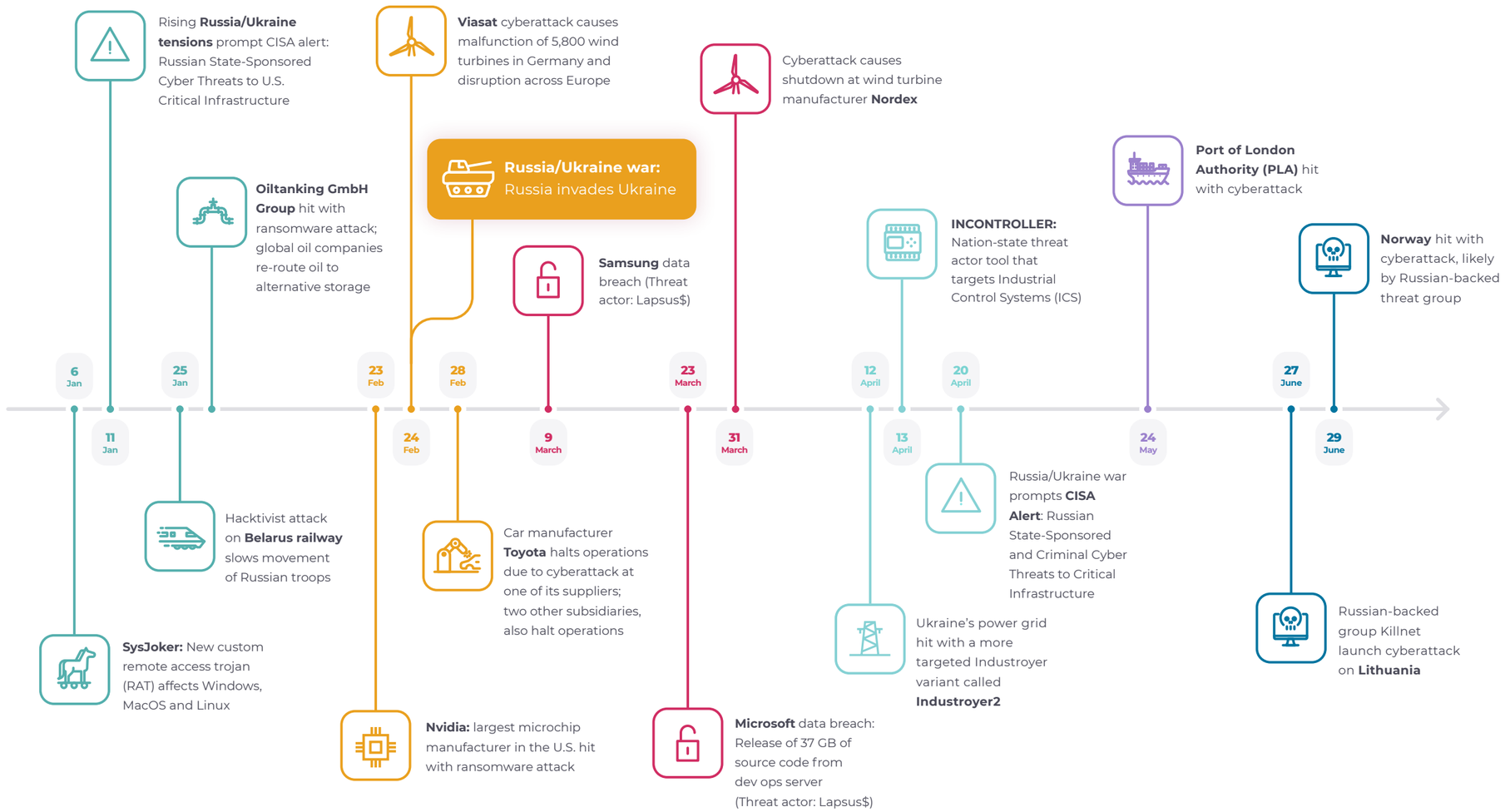
Industroyer2

Timeline of Notable Cyber Events in the First Half of 2022

The timeline on this page highlights several significant cyber events between January and June 2022 that have shaped the current threat landscape.

Since Russia began its invasion of Ukraine in February 2022, we have seen activity from several types of threat actors, including hacktivists, state backed APTs and cyber criminals.

We also saw robust usage of wiper malware, and an Industroyer variant, dubbed Industroyer2, was developed to misuse the IEC-104 protocol, which is commonly used in industrial environments.



IoT Botnet Landscape

Nozomi Networks Labs' honeypots collect data that, when analyzed, provides some interesting insights into threat actor activity. In the first half of 2022, we observed the following trends:

- **Top attacker countries:** Top cyber activity comes from IP addresses associated with China and the United States. Their attack surfaces are likely increased due to their sophisticated tech and manufacturing industries.
- **Protocols involving hard coded credentials:** Mirai is a popular botnet that originally misused Telnet but since threat actors released the source code to the public, it has been modified to target SSH and other protocols.
- **Top credentials used:** "root" and "admin" credentials are obvious attractive targets used in multiple variations as they may allow threat actors to access all system commands and user accounts.
- **Top number of unique attacker IP addresses:** As our honeypots collected IP addresses associated with malicious activity, March was the most active month with close to 5,000 unique attacker IP addresses collected.
- **Top executed commands:** We identified the top 10 executed commands with `enable`, `shell`, `system` and `which ls` making the list. Roughly 12,500 bots executed each of these commands.

March
was the most active month for botnets with close to

5,000
unique attacker IP addresses collected.

Read the **Full Report** to learn more about IoT botnet activity in the first half of 2022.

The Vulnerability Landscape

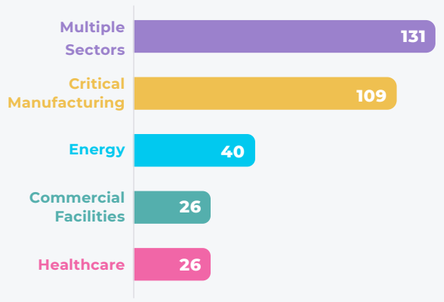
The security posture of many ICS software and hardware products is exposed through vulnerabilities discovered mostly by security researchers. In the first half of 2022, there were 560 ICS-CERT-issued Common Vulnerabilities and Exposures (CVEs), of which 303 were newly announced in 2022. There were 14% fewer CVEs reported compared to the second half of 2021.

Of the reported CVEs, 131 affected multiple sectors. Critical manufacturing was the most directly impacted sector with 109 reported CVEs. Energy followed with 40, and healthcare and commercial facilities both came in third with 26. Additionally, 60 different vendors were mentioned in CVE advisories, with 172 associated products. Affected vendors were up 27% and affected products up 19% from the second half of 2021.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

560
CVEs issued

MOST IMPACTED INDUSTRIES



Recommendations

There is a growing need to take proactive security measures that can be implemented by different stakeholders within an organization. This includes IT teams, compliance officers and risk managers who may have different perspectives on security issues. Priority security practices should include:

- Maintaining an accurate asset inventory
- Implementing the latest patches on VPN technology
- Privileged access management
- Using strong Multi-Factor Authentication (MFA) that is not susceptible to vishing or SIM swapping
- Frequent password changes, and
- Increased employee training on vishing and overall social engineering

Additional mitigations:

- **Backups:** To ensure that a ransomware or wiper malware attack does not result in a complete data loss, back up your data regularly, test your backup system, and ensure that your backup is stored in an off-site location and not on the same network as operational servers.
- **Threat Intelligence:** Cyber threat intelligence is the practice of collecting, analyzing, and disseminating information about cyber threats to help organizations protect their systems and data. This information can include malware signatures, attack vectors, and indicators of compromise (IoC)s.
- **Cloud Security:** Ensure that your cloud provider has a solid reputation and is compliant with industry standards like ISO 27001 or SOC 1/2/3 certifications, encrypts data when being stored or transferred, and uses 2FA and identity management tools.
- **Threat Detection:** Threat detection is used to detect and respond to potential threats in real time, as well as provide alerts for future events. In threat detection, systems monitor the network for suspicious activities, such as an unusual amount of traffic coming from one IP address, or a large number of connections being made to a particular service. This can be done by watching for abnormal activity over time or by scanning the network for known vulnerabilities.
- **Software Bill of Materials (SBOM):** The SBOM gives you an idea of how many different versions of each component exist and where they are used, so you can track changes over time and make sure they do not cause problems with other components. It can also help you understand which components are more exposed or more vulnerable than others, and how to mitigate those vulnerabilities. While SBOMs are not yet widely used, it is worth monitoring the development of this technology.

KEY THREAT MITIGATIONS FOR STRONGER SECURITY

Forecast

Based on this latest analysis, below are some of the key cybersecurity trends we expect to see throughout the rest of 2022:

- More ICS-related attacks
- Ransomware threat actors will continue to target critical infrastructure companies
- More attacks targeting larger companies
- Theft of tech source code
- An increase in cyber policies and governance as private/government initiatives established earlier this year take form

Download the OT/IoT Security Report

Nozomi Networks Labs analyzes the current threat landscape and shares:

- Recent ransomware and IoT botnet attacks
- ICS, OT/IoT device vulnerability and exploitation trends
- Steps to improve your cyber threat remediation strategies

Download

NOZOMI NETWORKS

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NN-SEC-RP-ES-2022-1H-001

nozominetworks.com