NOZOMI NETWORKS LABS

RESEARCH REPORT

OT/IoT Security Report

Cyber War Insights, Threats and Trends, Recommendations

2022 1H Review | August 2022

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/labs**

Table of Contents

1. Introduction 4

2. The Threat Landscape 6
   - 2.1 Who is Lapsus$ and Why Should You Be Concerned? 7
   - 2.2 Russia/Ukraine War Spikes Cyber Activity 9

3. The IoT Botnet Landscape 12
   - 3.1 Protocols Involving Hard Coded Credentials 13
   - 3.2 Top Attacker Countries 14
   - 3.3 Top Credentials Used 15
   - 3.4 Top Number of Unique Attacker IPs 16
   - 3.5 Top Attacker IP Addresses 17
   - 3.6 Top Executed Commands 18

4. The Vulnerability Threat Landscape 19
   - 4.1 Analysis of ICS-CERT Advisories 20

5. Recommendations 22
   - 5.1 Expert Recommendations 23

6. Forecast 25
   - 6.1 What to Expect in the Remainder of 2022 26

7. References 27

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 changing, and at a more rapid pace than ever. From cyber threat activity incited by the Russia/Ukraine war to threat actors obfuscating their malicious activity, attacks can be unpredictable. Threat actors have changed their tactics, focused on new targets, and increased their attack frequency.

Meanwhile, companies are fighting the endless battle of making industrial processes more efficient without compromising security.

In the past, insights into threats and trends proved beneficial in helping companies strengthen security and minimize future threats. For example, in 2020 the shift to work from home (WFH) policies due to COVID-19 caused an increased targeting of Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) vulnerabilities. While companies focused their defense strategies on educating employees about network security (since they no longer had autonomy over their corporate networks), vendors continuously released patches for end users to implement. As another example, in **2021** when ransomware attacks were on the rise, there was a fixation on software supply chain compromises. This led to ransomware resilience strategies, supply chain security, and the introduction of government initiatives focused on securing critical infrastructure. This begs the question: In the first half of 2022, what trends are we, Nozomi Networks Labs, seeing and how can companies use these insights to tailor their cybersecurity strategies? This report shares our analysis and observations. It is a more in-depth addition to the blogs and white papers we publish.

To help security teams and researchers of OT/IoT environments, this report focuses on three main areas:

- **Attack trends**
- **Vulnerability research**
- **Recommendations**

We recap the Russia/Ukraine crisis, highlighting newly introduced malicious tools and malwares, as well as how this conflict can give us insights into attacker capabilities.

We also provide insights into IoT botnets, corresponding Indicators of Compromise (IoCs) and threat actor Tactics Techniques and Procedures (TTPs). We conclude with recommendations for mitigating threats and forecasting analysis of what to expect throughout the rest of 2022.

REPORT INSIGHTS

Russia/Ukraine crisis
- New malicious tools and malwares
- Insights into attacker capabilities

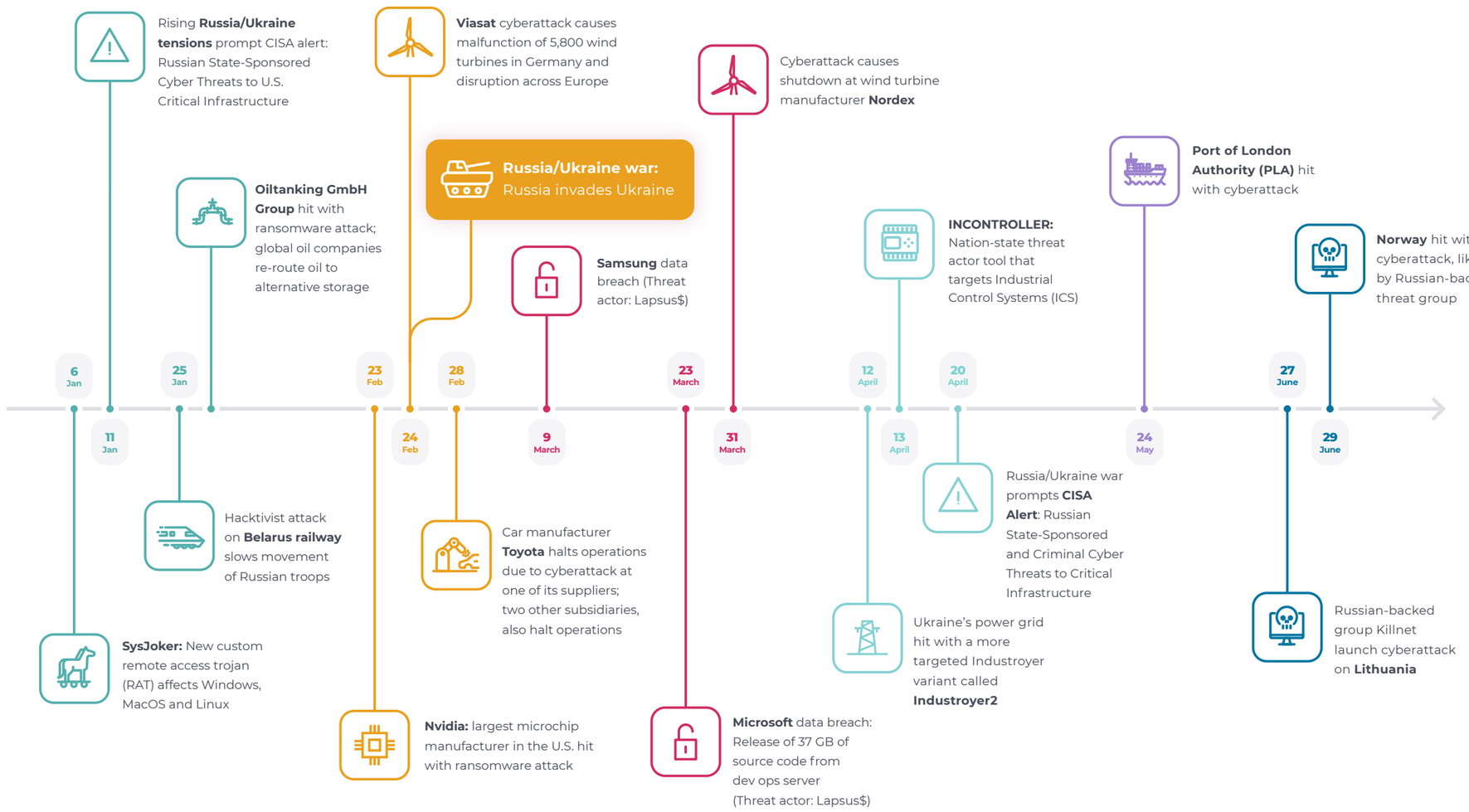
IoT botnets
- Indicators of Compromise (IoCs)
- Threat actor Tactics Techniques and Procedures (TTPs)

Recommendations and forecasting
- Key threat mitigations for stronger security
- Analysis of what to expect throughout the rest of 2022

Timeline of Notable Cyber Events in the First Half of 2022

This timeline highlights several significant cyber events between January and June 2022 that have helped shape the current threat landscape.

Since **Russia** invaded 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 use of **wiper malware**, and an Industroyer variant, dubbed **Industroyer2**, was developed to misuse the IEC-104 protocol, which is commonly used in industrial environments.



2

The Threat Landscape

2.1 Who is Lapsus$ and Why Should You Be Concerned? 7

2.1.1 Nvidia 8

2.1.2 Samsung 8

2.1.2 Microsoft 8

2.2 Russia/Ukraine War Spikes Cyber Activity 9

2.2.1 Belarus Railway Hacktivism 10

2.2.2 ViaSat Cyberattack 10

2.2.3 Wipers & Wartime 10

2.2.4 INCONTROLLER 11

2.2.5 Industroyer2 11

2.1 Who is Lapsus$ and Why Should You Be Concerned?

The 2022 cyber threat landscape is a complex one, with multiple factors contributing to the risks of a breach or cyber-physical attack.

These include:

- **The increasing number of connected devices**
- **The growing sophistication of malicious actors**
- **The increased reliance on cloud services and data sharing**
- **The escalation in attacks against critical infrastructure and enterprises that are using industrial control systems (ICS)**

As the threat landscape continues to evolve, organizations must keep pace with technology and new threats to protect their assets. From January to June 2022, we observed trends in wiper malware being used, threat actors obfuscating their activity, and increased APT activity during the Russia/ Ukraine crisis that puts critical infrastructure at risk. In this section, we will take a closer look at how cyber threats have evolved over time, who is behind them, and what you can do to protect yourself against them.

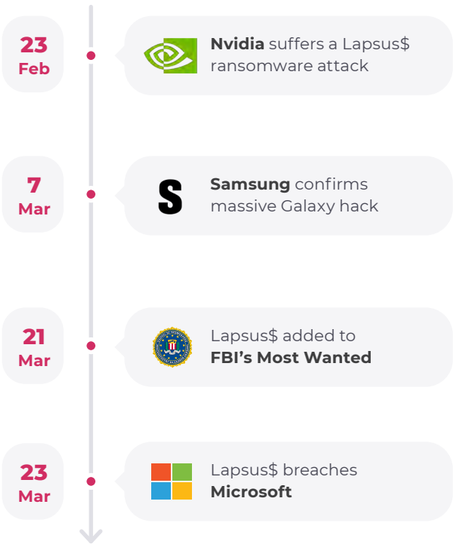
On March 21, 2022, the United States Federal Bureau of Investigation (FBI) added the Lapsus$ threat group to the Most Wanted list for "Cyber Intrusions of United States-Based Technology Companies."[1] Lapsus$ is responsible for several high-level cyberattacks between the months of February and March of 2022, including attacks on Nvidia, Samsung, and Microsoft.

Although Lapsus$ is not necessarily considered a ransomware group, they have found a way to monetize their findings by demanding money from victims in exchange for not disclosing or selling their data. They do not use traditional ransomware, nor do they try to restrict the victim's access to their files, so victims operate as normal.

This is concerning because data breaches take less skill and effort to carry out, since there is no associated ransomware to deploy on the network to encrypt files.

This has enabled the threat group to launch multiple large-scale attacks within a few months.

Lapsus$ attacks in the First Half of 2022



Following is a summary of Lapsus$-related attacks between January and June 2022.

2.1.1 Nvidia

Microchip manufacturer Nvidia, inventor of the graphics processing unit (GPU) suffered a ransomware attack on February 23, 2022. The threat group claimed to steal 1 TB of data, including company Intellectual Property (IP) and Personally Identifiable Information (PII) belonging to 71,000 employees.[3] Lapsus$ threatened to leak sensitive information unless certain demands were met. However, because this was not a ransomware attack and the victim did not experience any interruptions, Nvidia was able to continue operating as normal. Details on the sensitivity of the leaked information are not yet known.

2.1.2 Samsung

Threat actors stole 190 GB of confidential code, Galaxy biometric authentication algorithms, and bootloader source code for Galaxy phones.[4] These software programs help load other software onto computers.

2.1.2 Microsoft

Lapsus$, tracked by the Microsoft Security Team as DEV-0537, breached Microsoft on March 23, 2022. Before the threat actors could use the compromised account to escalate privileges, the Microsoft team was able to stop them in their tracks and prevent further activity. Although the threat actors were able to steal source code of the Azure DevOps server, Microsoft has assured that it "does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk."[5]

For additional information on Lapsus$ (DEV-0537) TTPs and details on mitigations, read the full Microsoft report here.

According to Microsoft,[2] the threat actor does not try to obfuscate activity and uses the following TTPs to carry out attacks:

- Vishing
- Social engineering
- Using third-party relationships
- SIM-swapping
- Accessing VPNs
- Paying insiders for access
- Using password stealers
- Using exposed credentials found in public code archives

2.2 Russia/Ukraine War Spikes Cyber Activity

International conflict often incites cyber threat activity, and the Russia/Ukraine war is no exception. Nation-state actors have been involved in cyber campaigns against Ukraine since 2015, using malware such as BlackEnergy and NotPetya to cause significant disruption to critical infrastructure sectors including power generation and distribution. After Russia invaded Ukraine in February 2022, we witnessed an emergence of malicious tools specifically targeting OT technology.

It is clear that cyberattacks have become a force multiplier during conflict.

We are seeing various cyber actors, malicious tools (ransomware, wipers, ICS malware) operating simultaneously in the threat landscape.

Here is what we can learn from this war:

- **War increases cyber activity:** Of the varying threat actors and motives, nation-state Advanced Persistent Threats (APTs) are the most active during wartime. They are less financially motivated and more focused on cyber espionage—spying and disrupting communications and other critical enemy systems.

  Some companies become incidental casualties of cyber war as a result of threat actors' attacks on their targets.

- **Private companies are stakeholders in war:** In addition to military and government entities, private companies, especially critical infrastructure companies (manufacturing, communications, transportation, energy, etc.) are also prime targets during wartime.

  Companies should maintain a heightened security posture and cooperate with their governments to safeguard assets in the event of a war.

- **Wartime contingency and data security strategies are necessary:** Ukrainians relocated their sensitive servers out of the country in case a physical attack was launched on their communications infrastructure. An attack on in-country servers could prevent Ukrainians from organizing efforts with domestic troops and even allies, putting them at a disadvantage during the war.

  There is a need for a data protection strategy during wartime, whether it be **backing up data** to the cloud prior to war, or establishing a process to relocate servers to designated areas out of country and in a specified timeframe, etc.

  While this will not necessarily prevent a cyberattack on those servers, it will safeguard them from being destroyed through a physical attack in-country. Hacktivist groups, cyber criminals, and nation-state threat actors have launched successful cyberattacks on critical infrastructure companies, directly or indirectly, because of the Russia/Ukraine war.

The following sections give examples of Russian cyber incidents we have observed so far this year.

2.2.1 Belarus Railway Hacktivism

On January 25th, a Belarusian hacktivist group successfully attacked the state-run railway server to disrupt Russian troop activity throughout the country. The attack was launched in protest of the Belarusian government's support of Russia.[6] The government was attempting to aid Russian war efforts by moving troops and weapons via railroad to provide strategic access into Ukraine.

2.2.2 ViaSat Cyberattack

Global communications company Viasat was hit with a cyberattack on February 24, 2022, the same day Russia invaded Ukraine. The attack impacted thousands of Viasat customers. Several consumer-oriented modems, the majority located in Ukraine and others in Europe, were gradually knocked offline for 45 minutes.

Based on forensics investigations, it appears that the attackers were able to use a KA-SAT management mechanism to simultaneously deploy a destructive payload to multiple KA-SAT modems. The payload rendered the modems unable to connect back to the network by wiping their flash memory.

A notable spillover effect of this cyberattack was loss of view of Enercon's 5,800 wind turbines in Germany, which could no longer be remotely monitored.[7,8,9] ViaSat later confirmed that the AcidRain wiper caused the disruptions, thus beginning the influx of wiper malware used during the Russia/Ukraine war.

2.2.3 Wipers & Wartime

A wiper is a type of malware that erases all data or renders it useless. Wipers are often used in cyber warfare, with the intention of causing an enemy to lose access to critical data. A wiper can be seen as a type of self-replicating malware, but it does not need to spread from one machine to another like most viruses do. Instead, wipers typically seek out specific files and delete them from the hard drive completely.

On February 26, 2022, CISA published Alert AA22-057A[10] describing the types of destructive malware used to target various organizations in Ukraine, rendering computer systems inoperable. The wipers described in the alert are:

- **HermeticWiper:** HermeticWiper overwrites the master boot record, rendering the operating system unable to boot. HermeticWiper was used in conjunction with HermeticWizard, which provided worm functionality to spread HermeticWiper across entire networks.[11]
- **IsaacWiper:** IsaacWiper, also used in conjunction with Hermetic Wizard, overwrites user files with random data, rendering any attached storage disk unusable.[12]
- **CaddyWiper:** CaddyWiper works similarly to other wipers. Not only does it attempt to replace victim files with "null" data, but it also then attempts to wipe the master boot record (MBR), corrupting the victim's stored data.[13, 14, 15]
- **WhisperGate:** In January 2022, Microsoft Threat Intelligence Center (MSTIC) discovered this wiper. As the above wipers, it aims to erase data, rendering devices inoperable.

As previously discussed in relation to the Viasat cyberattack, the AcidRain wiper operates in the typical fashion by wiping victim data which leads to disruption of business and industrial processes. If a computer contains multiple drives—such as one for storing personal files and another for storing digital backups—the wiper could also destroy all copies of those files stored on external devices like USB sticks or network drives.

Wipers have become popular among nation-state APTs who are not necessarily financially motivated but instead want to cause as much destruction as possible.

2.2.4 INCONTROLLER

On April 13, 2022, CISA released Alert AA22-103A warning of malicious tools targeting ICS.[16] According to this alert, threat actors have the ability to gain full access to supervisory control and data acquisition (SCADA) and other ICS including Schneider Electric, OMRON Sysmac NEX PLCs and vOpen Platform Communications Unified Architecture (OPC UA) servers.

The report also warned that threat actors target engineering workstations running Windows, exploiting the CVE-2020-15369 (aka ASRock vulnerability) which leverages the HMI in SCADA systems.

NOZOMI NETWORKS BLOG

INCONTROLLER: Acting to Protect Customers from Unknown Threats

According to information from our partner Mandiant, INCONTROLLER is believed to have been developed by a sophisticated nation-state threat actor to maliciously manipulate ICS environments. So far INCONTROLLER has not been tied to any incident, nor to a specific threat actor.

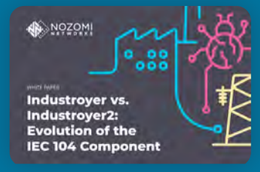
Read More ›

2.2.5 Industroyer2

The emergence of Industroyer2 proved that threat actors still have the ability to actively update potent malware or craft custom payloads to meet operational requirements. There have been reports of some hardcoded IPs in the malware sample, which is an indication that the threat actors had intimate knowledge of the environment in which they were deploying it.

Russian APT Sandworm developed a variant of the Industroyer malware used in the 2015 attack on Ukraine; Industroyer2 specifically targets the IEC 104 protocol. Given the similarities in the Industroyer and Industroyer2 source code, it is possible that Sandworm is using Industroyer as a broader framework to create future variants that specifically target other ICS protocols. Network anomaly detection and hunting for suspicious events can potentially help to discover such attackers early on.

WHITE PAPER



Industroyer vs. Industroyer2: Evolution of the IEC 104 Component

In this analysis of Industroyer2 from Nozomi Networks Labs, learn about its OT capabilities, major changes between Industroyer and Industroyer2, and how the codebase has evolved over time.

Read More ›

Download Our Content Pack for Protections ›

NOZOMI NETWORKS

3

The IoT Botnet Landscape

3.1 Protocols Involving Hard Coded Credentials 13
3.2 Top Attacker Countries 14
3.3 Top Credentials Used 15
3.4 Top Number of Unique Attacker IPs 16
3.5 Top Attacker IP Addresses 17
3.6 Top Executed Commands 18

3.1 Protocols Involving Hard Coded Credentials

In this chapter we share unique data collected by Nozomi Networks Labs. These insights can help companies understand how threat actors are targeting and accessing networks.

Despite SSH being the secure communications alternative, Telnet is still widely used today. Both allow network administrators to remotely access devices connected to a network. This makes Telnet and SSH primary targets for threat actors looking to gain remote access. Historically, many IoT devices have been shipped with weak default credentials that, once guessed, give attackers access to them.

Figure 1 shows how Telnet and SSH were almost equally targeted throughout the first half of 2022, with Telnet at 51% and SSH at 49%.

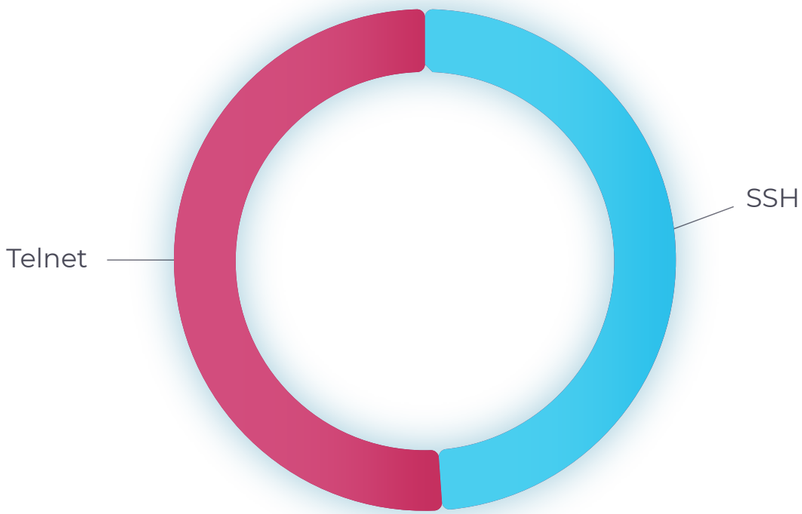


Figure 1: *Protocols involving hard coded credentials, January-June 2022.*

INSIGHTS

Although **SSH is more secure**, threat actors can use brute force or other tactics to obtain embedded credentials.

Additionally, **Mirai** is a popular botnet that originally misused Telnet but once threat actors released its source code to the public, it was manipulated to target SSH and other protocols.

3.2 Top Attacker Countries

As the world becomes more interconnected through technology, it becomes increasingly difficult to pinpoint exactly where a cyberattack originated. The use of multiple computers and servers by attackers makes it even more challenging to attribute cyberattacks.

Figure 2 shows the top countries where compromised devices are leveraged by attackers to launch cyberattacks. The most activity in the first six months of 2022 came from systems located in China and the United States.

Although this chart shows that U.S. and China are the top attacker countries, there is not always a direct correlation between the location where the cyber activity originates and the location of the threat actor, as servers anywhere in the world can be leveraged to carry out global cyberattacks.

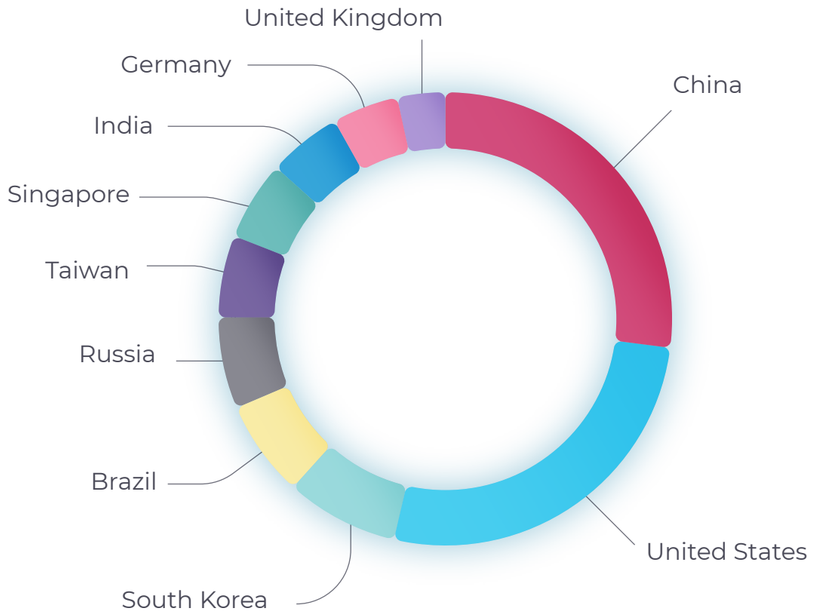


Figure 2: *Top countries where compromised devices are used to execute attacks January-June 2022.*

INSIGHTS

Top Attacker Countries

China

United States

Possible Reasons

- The attack surfaces of China and the U.S. are larger due to their sophisticated tech and manufacturing industries.
- The number of connected devices increases the number of vulnerable devices susceptible to exploits.
- Since some of the affected systems may be hosted in the cloud, and most of the top cloud providers are based in the U.S., the U.S. will logically lead in terms of numbers.

3.3 Top Credentials Used

One of the main ways threat actors gain initial access into IoT is by using default credentials to access systems. Because many companies don't change default passwords in their software, threat actors are able to access the network undetected because the access is coming from legitimate credentials and won't necessarily generate alerts.

Figure 3 shows the top default usernames and passwords that threat actors use to gain initial access. "nproc:nproc" username and password were the most used credentials to access IoT networks reported by our honeypots, with almost 12,000 associated attempts recorded. "root" and "admin" credentials are obvious attractive targets used in multiple variations as they may allow threat actors access to all system commands and user accounts.

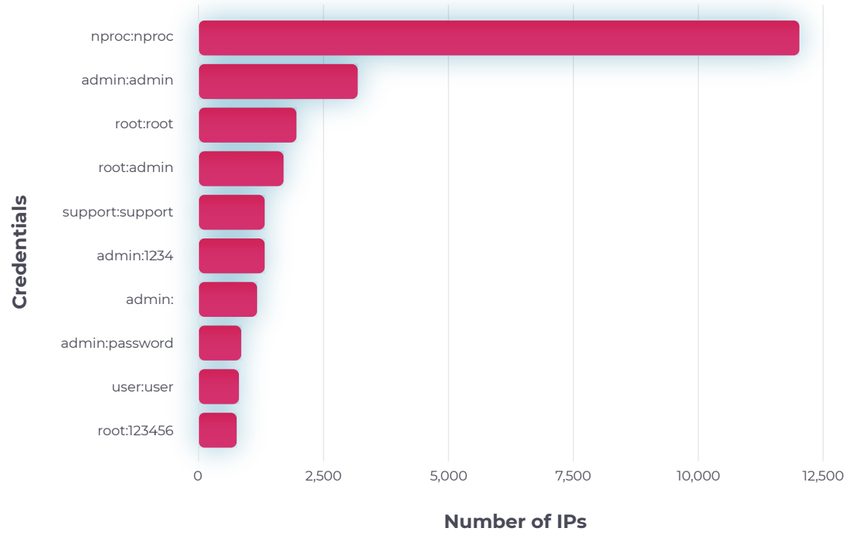


Figure 3: *Top credentials used January-June 2022.*

INSIGHTS

The two values seen in most of the credential variations recorded are:

admin
and root

Reasons

- Device manufacturers commonly use them to provide maximum unrestricted access to vulnerable devices for troubleshooting purposes.
- From the attackers' perspective, these options are particularly beneficial as they are already associated with high privileges, making privilege escalation unnecessary.

3.4 Top Number of Unique Attacker IPs

We define “unique” as non-repetitive Indicators of Compromise (IoCs) collected by Nozomi Networks Labs honeypots. Figure 4 shows the number of unique attacker IPs that have targeted OT/IoT networks between January and June.

In late March, we recorded almost 5,000 unique values associated with malicious activity, the highest number during this period.

Figure 4: *Unique attacker IPs January-June 2022.*

INSIGHTS

With threat intel teams **constantly blocking malicious IPs and URLs,** threat actors continue to use new IoCs to increase their chances of success.

We noticed a **significant increase in February** (during severely heightened tensions prior to Russia invading Ukraine), however there is not enough evidence to correlate the Russia/Ukraine war with this activity.

3.5 Top Attacker IP Addresses

On the right are the IP addresses discovered in IoT, with the top entry associated with over 30,000 access attempts.

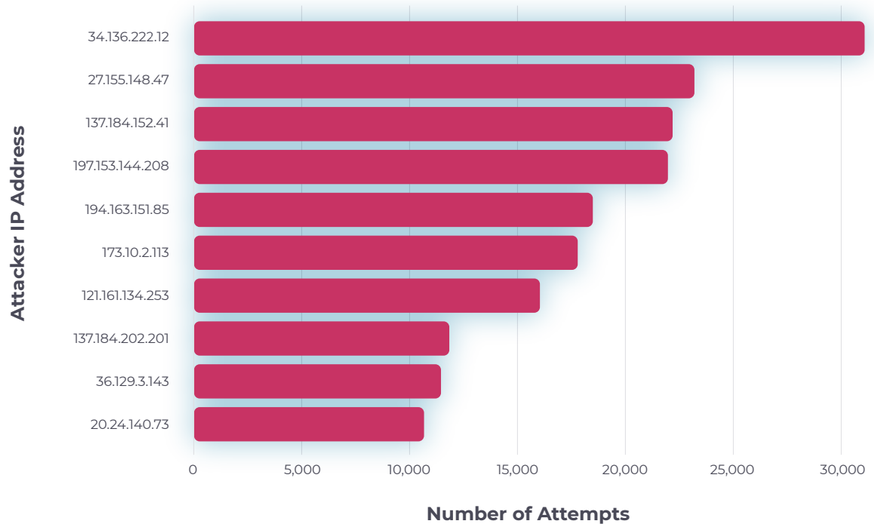


Figure 5: *Top attacker IPs January-June 2022*

INSIGHTS

Although we collect various IPs associated with malicious activity, there's a possibility **threat actors could leverage legitimate IPs** to make IR and forensics difficult.

We recommend using **dedicated threat intelligence feeds** to identify the source and origin of malicious IP addresses.

3.6 Top Executed Commands

Once initial access is obtained, threat actors execute commands on a system that will allow them to maintain persistent and escalate privileges. Figure 6 shows the top executed commands from January through June 2022.

Roughly 12,500 bots executed each of these commands. This graph provides insight into the most common commands used by threat actors when maneuvering throughout a network.

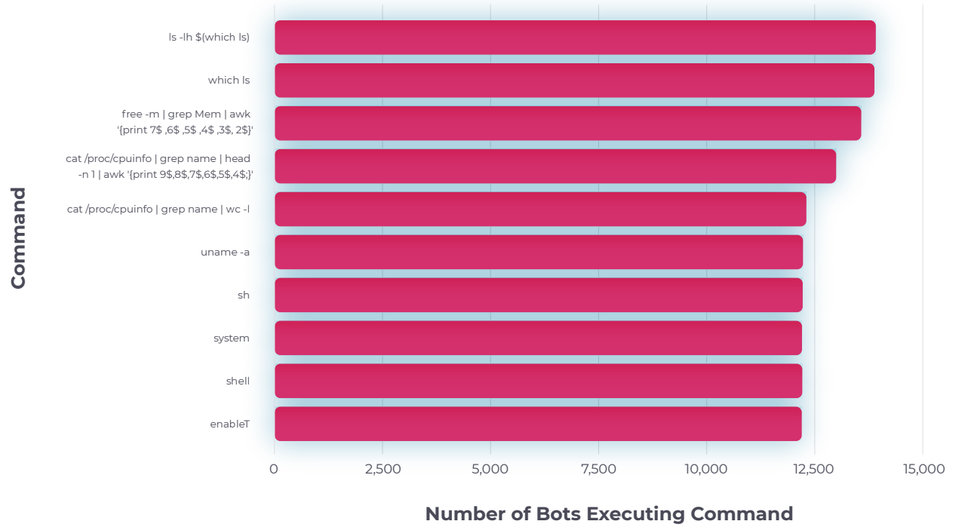


Figure 6: *Top executed commands January-June 2022.*

INSIGHTS

The **`enable`** and **`shell`** commands allow for the OS to process all other malicious commands, while **`system`** command carries out the command in the processing center. **`uname -a`** command is used to pull up system information on the target machine.

The **`which ls`** command is used to locate executable files.

4

The Vulnerability Threat Landscape

4.1 Analysis of ICS-CERT Advisories **20**

4.1.1 Number of CVEs Released in 2022 by Sector 20

4.1 Analysis of ICS-CERT Advisories

On the right is analysis of ICS-CERT advisories from the first half of 2022.

From January – June 2022, there were 560 Common Vulnerabilities and Exposures (CVEs) released, of which 303 were newly announced in 2022. There were 60 affected vendors mentioned in these advisories, with 172 associated products.

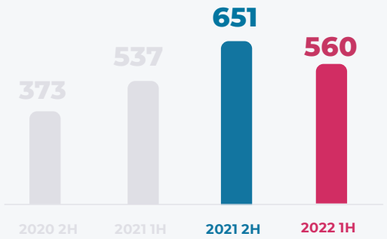
CVE reporting was down by 14% compared to the second half of 2021, while mentioned vendors went up 27% and affected products up 19% from the second half of 2021.

4.1.1 Number of CVEs Released in 2022 by Sector

Although 131 reported CVEs affected multiple sectors, 109 directly affected critical manufacturing, followed by energy and healthcare. It is worth mentioning that in many cases the same vulnerability affects several industries.

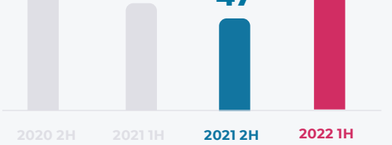
Total ICS-CERT Vulnerabilities Disclosed

-14% decrease



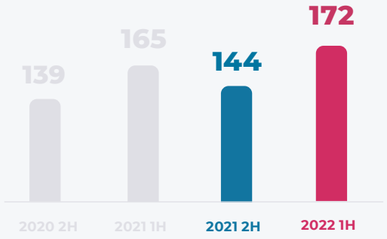
Total Vendors Affected by Disclosed Vulnerabilities

+27% increase

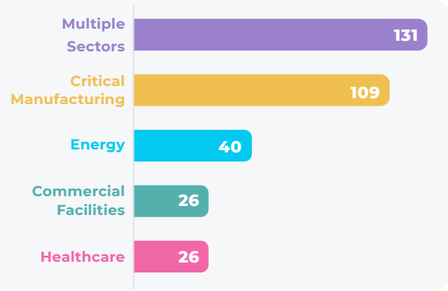


Total Products Affected by Disclosed Vulnerabilities

+19% increase



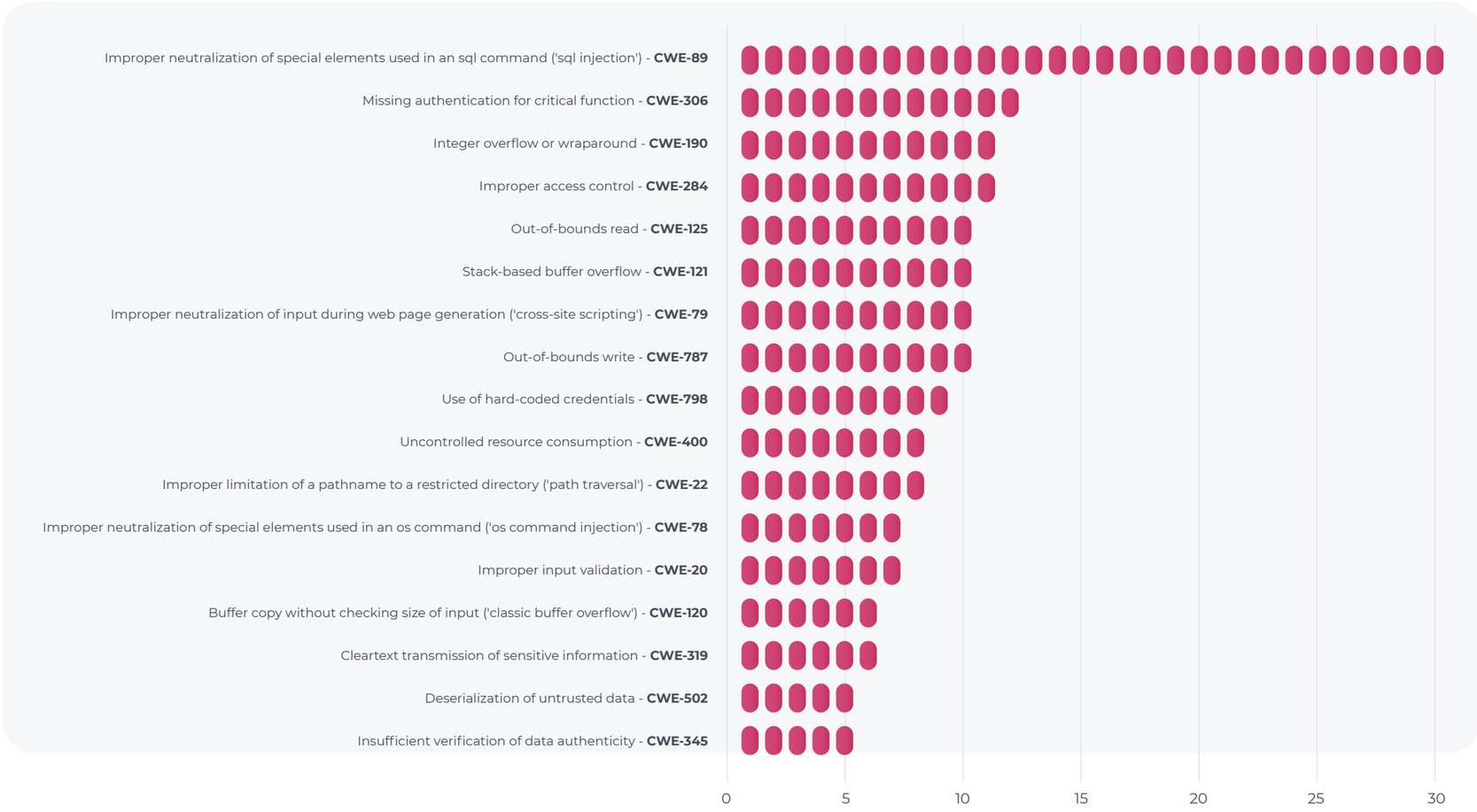
Top 5 Sectors Affected by Disclosed Vulnerabilities



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

As we can see, SQL injections top the chart for the ICS field, having the highest number of associated vulnerabilities reported in 2022. Other most reported critical weaknesses include misused authentication, improper access controls, and integer overflow vulnerabilities.

Number of CWEs Associated with CVEs, January-June 2022



5 Recommendations

5.1 Expert Recommendations **23**

5.1.1 Backups 23

5.1.2 Cyber Threat Intelligence (CTI) 23

5.1.3 Cloud Security 24

5.1.4 Threat Detection 24

5.1.5 Software Bill of Materials (SBOM) 24

5.1 Expert Recommendations

The industrial security cyber threat landscape is changing at a rapid pace. As companies explore the possibilities of more efficient operations, they are finding themselves in a constant battle between security and efficiency. As a result, organizations need to be able to quickly adapt to new threats and trends to remain secure. This means that traditional security methods are no longer sufficient as they do not allow organizations to react quickly enough or provide sufficient context for them to make informed decisions. There is also a growing need for actionable intelligence that can be used by different stakeholders within an organization such as IT teams, compliance officers and risk managers who may have different perspectives on security issues. This includes:

- **Deploying asset intelligence**
- **Using privileged access management**
- **Implementing the latest patches to VPN technology**
- **Using strong Multi-factor authentication (MFA) not susceptible to vishing or SIM swapping**
- **Making frequent password changes**
- **Increasing employee training on vishing and overall social engineering**

In addition to the above cyber hygiene, below are some key strategies for dealing with cybersecurity threats and staying ahead of emerging threats in 2022 and beyond.

5.1.1 Backups

It is essential for companies to have robust backups. This will ensure that a ransomware or wiper malware attack does not result in a complete data loss. Back up your data regularly and test your backup system. Ensure that your backup is stored in an off-site location, and not on the same network as operational servers, to ensure maximum protection from ransomware and malware attacks.

This ensures that your backups are protected from both physical and cyber attacks by threat actors who want to destroy data, but also ensures that they can be easily accessed when needed.

5.1.2 Cyber Threat Intelligence (CTI)

Cyber threat intelligence (CTI) 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.

The challenge of identifying the source of an attack has been compounded by the fact that many organizations continue to rely on outdated security solutions that lack visibility into their environments, thus hindering their ability to identify anomalies and prioritize remediation efforts. Threat intelligence can help you understand what types of attacks have occurred historically as well as what types have been successful in breaching systems or destroying data.

Cyber threat intelligence is essential for effective cybersecurity—but it is also a difficult task. There are many different types of threats, ranging from various trojans (and their variants) to social engineering attacks and DDoS attacks. Each requires its own approach to collecting and analyzing data. Cyber threat intelligence benefits include:

- Identifying active threats to your organization's security posture
- Identifying adversaries conducting reconnaissance on your organization's systems and data
- Understanding adversary tradecraft for use in future incident response engagements

5.1.3 Cloud Security

Cloud security is a growing concern for businesses. While cloud computing can be a great way to save money, it also means that your data is stored on someone else's servers and may be accessed by people you don't know. This can leave your company vulnerable to breaches and attacks that could shut down your business. Threat actors gain unauthorized access to the cloud service provider's (CSP) network or computers by exploiting flaws.

Robust cloud security can be achieved through the following steps:

- Ensure that the cloud provider has a solid reputation and is compliant with industry standards like ISO 27001 or SOC 1/2/3 certification. You also need to ensure they have strong physical controls, like video surveillance and biometric authentication, as well as software controls, like firewalls and intrusion detection systems
- Ensure that your data is encrypted when it is being stored or transferred
- Use identity management tools
- Use two-factor authentication (2FA) for logins
- Use firewalls to isolate networks from unauthorized access
- Monitor activity logs for suspicious activity
- Audit user accounts regularly

5.1.4 Threat Detection

Many threats can be difficult to detect and may cause damage before they are identified by an organization. Threat detection systems are 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.

5.1.5 Software Bill of Materials (SBOM)

A software bill of materials (SBOM) is a list of all the material components of your software product. It is used to track and manage your company's inventory, as well as to communicate with suppliers and customers.

A good SBOM should include:

- The name of the software being built
- A list of all components being used
- Optional details about each component (version, description, license)
- A historical log of when each component was added or removed

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 don't cause problems with other components.

It can also help you understand which components are more exposed or vulnerable than others, and how to mitigate those vulnerabilities. While SBOMs are not widely used today, it is worth monitoring the development of this technology.

6

Forecast

6.1 What to Expect in the Remainder of 2022

6.1 What to Expect in the Remainder of 2022

This forecast provides an overview of some of the key cybersecurity trends we expect to see throughout the rest of 2022.

1. Increase in ICS-related attacks and more sophisticated techniques.
As the Russia/Ukraine conflict persists, ransomware, lateral movement, and remote access tools are likely to see increasing use by threat actors to target ICS.

2. Ransomware threat actors will continue to view critical infrastructure companies as lucrative targets.
These companies are often more inclined to pay the ransom because they cannot afford disruptions in the OT environment.

3. More attacks will target larger companies.
Expect threat actors to aim for organizations with significant customer bases, sensitive customer data, and large revenues.

4. Theft of technology source code.
One of the biggest issues that businesses continue to face is not just the theft of PII, but also of tech source code. It can be used to develop targeted attacks designed to take down specific companies or industries.

5. More cyber policies and governance will be implemented.
As private/government initiatives established earlier this year take form, like CISA's JCDC, we will continue to see the effect they have in securing critical infrastructure.

7. References

[1] FBI, **"LAPSUS$ - Cyber Intrusions of United States-Based Technology Companies,"** March 21, 2022

[2] Microsoft Offensive Research & Security Engineering Team, **"DEV-0537 criminal actor targeting organizations for data exfiltration and destruction,"** Microsoft, March 22, 2022

[3] Sergiu Gatlan, **"NVIDIA data breach exposed credentials of over 71,000 employees,"** BleepingComputer, March 3, 2022

[4] Davey Winder, **"Samsung Confirms Massive Galaxy Hack After 190GB Data Torrent Shared Via Telegram,"** Forbes, March 8, 2022

[5] Microsoft Offensive Research & Security Engineering Team, **"DEV-0537 criminal actor targeting organizations for data exfiltration and destruction,"** Microsoft, March 22, 2022

[6] Phil Muncaster, **"Belarus Activists Fire Ransomware at State Railway,"** Infosecurity Magazine, January 25, 2022

[7] Juan Andrés Guerrero-Saade and Max van Amerongen, **"AcidRain | A Modem Wiper Rains Down on Europe,"** SentinelOne, March 31, 2022

[8] Viasat, **"KA-SAT Network cyber attack overview,"** March 30, 2022

[9] Maria Sheahan, Christoph Steitz and Andreas Rinke, **"Satellite outage knocks out thousands of Enercon's wind turbines,"** Reuters, February 28, 2022

[10] Cybersecurity & Infrastructure Security Agency, **"Alert (AA22-057A) Update: Destructive Malware Targeting Organizations in Ukraine,"** February 26, 2022

[11] Cybersecurity & Infrastructure Security Agency, **"Malware Analysis Report (AR22-115B),"** April 28, 2022

[12] Cybersecurity & Infrastructure Security Agency, **"Malware Analysis Report (AR22-115B),"** April 28, 2022

[13] Microsoft Offensive Research & Security Engineering Team, **"Destructive malware targeting Ukrainian organizations"** Microsoft, January 15, 2022

[14] Juan Andrés Guerrero-Saade, **"HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine,"** SentinelOne, February 23, 2022

[15] Welivesecurity, **"IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine,"** ESET Research, March 1, 2022

[16] Cybersecurity & Infrastructure Security Agency, **"Alert (AA22-103A) - APT Cyber Tools Targeting ICS/SCADA Devices,"** April 13, 2022

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-FULL-2022-1H-001

nozominetworks.com