RESEARCH REPORT

OT/IoT Security Report

Rising IoT Botnets and Shifting Ransomware Escalate Enterprise Risk

2020 1H

Table of Contents

1. Introduction

OT/IoT Security Report 2020 1H

The first six months of 2020 saw an increase in threats to OT and IoT networks, especially IoT botnet, ransomware and COVID-19-themed attacks.

These attack types align with global computing and socio-economic trends. The rapid rise in IoT devices and connections, the worldwide COVID-19 pandemic, and the increasing growth and sophistication of cyber criminals using ransomware for financial gain are the significant drivers.

This report provides an overview of the most active threats we saw in 1H, insight into their tactics and techniques, and recommendations for protecting your critical networks.

As an organization running critical infrastructure and automation networks, you are challenged as never before. You are dealing with ever increasing cyber threats, yet have a shortage of cybersecurity skills and inadequate OT/IoT threat detection tools and processes. Add to this major life and professional changes caused by the COVID-19 pandemic, including a workforce that now works primarily from home.

To help cybersecurity teams understand the evolving threat landscape and defend your systems, we are providing this review of the trends as they apply to OT and IoT security. It covers threats in the categories of IoT malware, ransomware, and COVID-19-themed attacks. We also summarize the top vulnerabilities exploited by threat actors in 1H.

New data from Juniper Research indicates that the total number of IoT connections will reach 83 billion by 2024,[1] representing a growth of 130% over the next four years. The industrial sector is expected to account for more than 70% of the connections in that period.

Mirroring this growth in devices, new and modified IoT botnet threats are one of the fastest growing categories of threats in the first half of 2020.

While the technical root causes are the same, the impact of an IoT botnet attack on consumer versus industrial devices is vastly different. An attack on a consumer gadget could be limited to a privacy issue, whereas the effect of a successful breach on a manufacturing device can have a significant production or safety cost.

THREATS TO OT SYSTEMS ARE RISING

2019 saw a 2,000% increase in incidents targeting operational technology (OT).

This could foretell the rising interest of threat actors in attacking industrial systems in 2020.

IBM Security[2]

Regarding ransomware, we expect to see a continued increase in targeted attacks that combine data encryption with data theft, an approach which was recently popularized by various ransomware families. Furthermore, recent examples of ransomware have started to exhibit OT-awareness (SNAKE, MegaCortex), meaning that

industrial control systems could possibly be targeted by non-state threat actors.

The COVID-19 pandemic has had a major impact on the global socio-economic environment. It has taken almost half a million lives and cost the global economy an estimated $9 trillion,[3] or up to 10% of global economic output. In terms of the threat landscape, it has provided threat actors with more vectors and opportunities for exploitation, in both computer systems and human psychology.

For example, many phishing campaigns are utilizing COVID-19 themes to trick targets into providing access to their systems. During the second week of April 2020, Google saw 18 million daily COVID-19 themed malicious emails.[4]

The level of risk associated with each of the threats described in this report depends on your organization's systems and security posture. While that is something only you can assess, this report provides insights and actionable recommendations to help you protect your networks.

IoT IS AN EASY AND PLENTIFUL TARGET FOR ATTACKERS

5.8 Billion

enterprise and automotive devices expected to be connected to the internet this year

Gartner[5]

98%

of all IoT device traffic is unencrypted

Palo Alto Networks[6]

57%

of IoT devices are vulnerable to medium or high severity attacks

2. Threat Landscape

2.1 IoT Malware

IoT malware threats are growing and will be an important component of the threat landscape for the foreseeable future. Several factors are contributing to this unprecedented growth, including:

- Exponential growth in the number of IoT devices.
- The insecure deployment of IoT devices that are directly accessible through the internet.
- A lack of security updates for IoT devices, leaving devices vulnerable to common (non-zero-day) exploits by many threat actors.
- The lack of visibility into IoT device security posture experienced by many asset owners.

Following are the most significant IoT malware we observed in the first half of 2020.

2.1.1 Mirai

The IoT botnet Mirai[7] came to prominence in 2H 2016. At its peak, it amassed over 600,000 IoT devices capable of attacking targeted networks with DDoS (Distributed Denial of Service) that reached a bandwidth of 1 Tbps.

When Mirai was publically released later that year, it unleashed a proliferation of variants that are still under development and very active in 2020.

Like Mirai, the variants propagate themselves using either Telnet default credentials or remote exploits for consumer devices, such as home routers, IP cameras and network-attached storage devices. The endgame for these types of malware historically has involved the use of these consumer-grade infected devices to perform DDoS attacks, or to mine cryptocurrency. However, today we are seeing a change in focus to enterprise attacks.

While variants use the same code base as the original Mirai blueprint, what differentiates them is the use of new remote exploits that broaden the spectrum of infected devices.

Due to the way these botnets propagate over time, different variants tend to target the same set of devices.

THE HISTORY AND IMPACT OF MIRAI

In 2016 the Mirai botnet was the first major cybersecurity attack that harnessed the power of compromised IoT devices to form a botnet of record-breaking power.

Mirai and its variants continue to lead the pack now setting their sights on large enterprises.

Cloudflare[7]

This means botnet attackers now must implement strategies to prevent a newly infected target from being compromised by a competing botnet.

2.1.2 Dark Nexus

Dark Nexus[8] is a botnet derived from Qbot and Mirai that was discovered in April 2020. The code development process for Dark Nexus is quite intriguing. Dark Nexus operators frequently issue new updates similar to releases you see with commercial software. Additionally, Dark Nexus operators brazenly hawk their DDoS mitigation services on the open internet.

Though Dark Nexus initially infected only a few thousand devices, defenders should keep an eye on this type of threat. Numbers can fluctuate quickly once a new remote exploit becomes available, as happened with Mukashi (described later in this report).

From a technical point of view, what stands out about Dark Nexus when compared to competing botnets is the elaborate mechanisms it uses to profile the processes running on the infected device. The goal of these mechanisms is to identify suspicious processes that might hinder the smooth execution of the malware.

NOZOMI NETWORKS BLOG

Dark Nexus IoT Botnet: Analyzing and Detecting its Network Activity

Nozomi Networks Labs analyzed the network behavior of several variants of Dark Nexus. They all leave a hefty network trail that can be broadly divided into three categories:

- C&C (command and control) communication
- Self-propagation
- DDoS attacks

We detail the actions and evidence left by Dark Nexus in each of the three areas of activity. We also provide a SNORT rule that be used by anyone in the security community to detect its traffic.

Nozomi Networks Labs[9]

2.1.3 Mukashi

Mukashi[10] is a new Mirai variant discovered in March 2020. It is the first malware to exploit the CVE-2020-9054 vulnerability at scale.[11] This pre-authentication command injection vulnerability was publicly released in February 2020, and it impacts ZyXEL network-attached storage (NAS) devices.

The speed at which a new exploit can be deployed and spread is a critical differentiator in this field, because it allows the botnet operator to compromise new targets before a competing botnet can.

2.1.4 LeetHozer

LeetHozer[12] is another example of malware that, while sharing similarities with Mirai, has several new features. On the technical side there are two noteworthy features.

The first is its targeting of Xiaongmai-based DVRs, NVRs and IP cameras, using a remote exploit that operates in two stages. Initially it sends a specially crafted packet to TCP port 9530 with the goal of starting the telnet daemon. Later, it leverages hardcoded credentials to login to the device through the newly spawned telnet service.

The second unusual feature of LeetHozer is the use of Tor to communicate with the C&C (command and control) server. While this is not the first time we have seen Tor in the context of malware, it is uncommon in world of IoT botnets.

2.1.5 Hoaxcalls

Hoaxcalls[13, 14] is an IoT malware discovered in April 2020, derived from Gafgyt/Bashlite. The characteristic that makes this bot remarkable is the frequent updates of exploits used for propagation.

When first analyzed, Hoaxcalls was embedding CVE-2020-8515 and CVE-2020-5722, two remote code execution vulnerabilities for CPE devices.

Later, new versions were found including:

- An exploit for an unpatched vulnerability for Zyxel Cloud CNM SecuManager, and
- A second exploit for Symantec Secure Web Gateway 5.0.2.8, a product that reached end-of-life in 2015.

2.1.6 Mozi.m

Mozi.m[15, 16] is a botnet that was first detected toward the end of 2019 and has remained very active throughout 1H 2020. It uses a DHT-based P2P (peer-to-peer) protocol for communication with the C&C, rather than a more traditional centralized client-server model.

The malware uses a digital signature to validate the messages sent by the bot master. Otherwise, any member of the P2P network could theoretically send commands to the other participants.

Using a P2P protocol for communication allows the bot management traffic to blend in with legitimate P2P network traffic. Another advantage is that there isn't a single point of failure that could be sinkholed.

DDoS attacks are the main attack functionality of Mozi.m and the network traffic generated by them is visible, even without sophisticated monitoring software.

2.2 IoT Malware Tactics and Techniques

To better classify and understand the general behavior of the threats discussed, we reference MITRE ATT&CK,[17] a public knowledgebase of tactics and techniques compiled from real world security data.

The **techniques used to gain an initial footprint on IoT devices** are very well understood and are categorized as follows:

2.2.1 ID: T1078 Valid Accounts

Attackers collect large sets of default valid credentials from device firmware. Sometimes the credentials have never been documented, or cannot be disabled by the end user.

2.2.2 ID: T1133 External Remote Services

Once a set of credentials has been embedded into IoT malware, the public internet is scanned to find services such as telnet or SSH. Once an open service is found, an attempt to login with the embedded credentials is performed.

2.2.3 ID: T1190 Exploit Public-Facing Application

IoT malware often relies on remote exploits for applications running on target devices. Given the lack of proper patch management procedures, attackers can be successful even without zero-day exploits.

Sometimes IoT botnet operators compete between themselves to be the first to infect a device by exploiting a given vulnerability. Then, they patch the security issue to exercise full, exclusive control of the newly acquired target.

Referencing the MITRE ATT&CK framework, **a common technique that essentially defines the IoT botnet category within the "Impact" tactic**, is:

2.2.4 ID: T1496 Resource Hijacking

In the past, IoT malware has been observed deploying cryptocurrency mining software. Today, this approach is not very common, presumably because IoT devices typically lack the significant computing resources required.

2.2.5 ID: T1498 Network Denial of Service (DDoS)

IoT botnets often have the capability to launch a synchronized DDoS attack against a specified network. The overall capacity of the attack is a factor of the number of devices multiplied by the bandwidth of each one.

2.2.6 ID: T1499 Endpoint Denial of Service (DDoS)

IoT malware can also target specific services such as web-based applications or DNS services.

2.3 Ransomware

Ransomware attacks targeting a variety of industry verticals remain commonplace. What is changing is the significance of the targets. Over the last year, one U.S. firm found that the average ransomware payment jumped **more than ten times to $302,539** across 950 incidents.[18] Ransomware gangs had shifted to focusing on larger, more critical targets with deeper pockets, including manufacturers, energy operators, local municipalities, and others.

Ransomware operators typically encrypt files and demand ransom payments from affected parties. Now they also exfiltrate company data and threaten to leak it publicly, as a way to apply more leverage.

While we do not have hard evidence confirming that this has increased success rates, more and more threat actors are adopting this tactic.

Another macro change in the ransomware world relates to the methods used to compromise targeted networks. While ransomware authors previously embedded code that performed automatic lateral movement, the new strategy has operators manually penetrating the target network. Once inside, they deploy ransomware exclusively on specific assets to cause the greatest disruption.

Although a manual network compromise might take longer, it can also be done in stealth mode. To successfully defend against this threat, defenders must carefully identify and monitor their most valuable assets.

2.3.1 Maze

Maze[19] is a prolific ransomware that has been around since 2019. Evidence suggests that it operates under an affiliate model, which explains the diversity in its targets as well as the heterogeneity in TTPs employed to successfully compromise its victims.

While originally spread through exploit kits and emails with malicious attachments, it has evolved to follow new trends and recently began to be deployed post-compromise. The post-compromise deployment approach gives the attackers time to perform lateral movement in the network and maximize the potential impact by exfiltrating and encrypting specific assets.

The organization behind Maze also operates a website where victims' exfiltrated data is displayed if the ransom is not paid.

What's quite unique about Maze in the current threat landscape is the way the operation is managed, its scale, and the sheer number of organizations that have become its victims.

MAZE RANSOMWARE TARGETS COVID-19 RESEARCH COMPANY

The Maze ransomware group attacked the computer systems of a UK-based medical research company on standby to carry out vaccine trials for the COVID-19 coronavirus.

The gang published personal details of thousands of former patients after the company declined to pay a ransom.

ComputerWeekly[20]

2.3.2 Ryuk

The Ryuk ransomware has been making headlines since 2018. Its operators primarily target major enterprises and have been responsible for many high-profile attacks. The infamous TrickBot and Emotet trojans have been seen distributing Ryuk payloads on compromised systems.

While several ransomware operators explicitly declared that they would suspend targeting organizations that were responding to the COVID-19 crisis,[21] the threat actors behind Ryuk continued to target healthcare providers.

2.3.3 Sodinokibi

Sodinokibi was responsible for several high-profile attacks, such as one in early 2020 that affected a foreign currency exchange company based in London.[22] The threat actor demanded $6 million to decrypt the affected files. The attack had a devastating impact on the continuity of the business, crippling many of its main activities for days, and ruining its reputation.

The organization behind Sodinokibi also recently set up a website where the stolen data was allegedly auctioned to the highest bidder.[23] This behavior is part of a more general trend where ransomware operators carefully analyze the exfiltrated data, aiming to maximize the value that can be extracted by any means.

RANSOMWARE PAYMENTS SOAR

Ransomware variants

like Ryuk, Maze and Sodinokibi are increasingly taking aim at large entities where attacks are customized to improve the odds of bagging a lucrative payout.

BakerHostetler[18]
The New York Times[24]

$1.1 million

was handed over by two Florida municipalities to pay off Ryuk attackers.

2.3.4 DoppelPaymer

Active since 2019, several variants of DoppelPaymer have recently been discovered. DoppelPaymer's codebase is believed to be derived from BitPaymer, although the two organizations continue to operate in parallel.

While DoppelPaymer has been used to successfully compromise companies in the energy sector, there is no evidence that it targets a specific industry. Rather, the organization responsible seems exclusively interested in finding high value victims.

In February, the group also released a publicly accessible website that exposed samples of victims' exfiltrated data, with the goal of extorting ransom.[25, 26]

2.3.5 SNAKE/EKANS

The SNAKE/EKANS ransomware raised security analysts' concerns in January 2020.[27] While not particularly advanced, this malware presented a "kill-list" of processes related to industrial automation software. The list was similar to an earlier one found on samples of the MegaCortex ransomware.

SNAKE/EKANS signals an important trend that sees ransomware operators targeting industrial control systems. At the time of writing, several successful publicly known attacks have utilized variants of the malware.

Matching a common characteristic of recent ransomware, SNAKE/EKANS also lacks an embedded propagation mechanism. Instead, it is expected to be run manually by the threat actor.

NOZOMI NETWORKS BLOG

Snake Ransomware is Raising Concerns for Industrial Controls Systems

A successful ransomware attack can be extremely debilitating, leaving victims with no other option than to meet the hackers' demands. To prevent that, it is important to have multiple controls in place to rapidly detect and block the threat. These include:

- Continuous security awareness training for employees
- Good network architecture with appropriate segmentation
- OT/IoT anomaly AND threat detection technologies.

Together, the techniques identify unusual behavior and context around suspicious activity, providing a fast start to response and remediation.

Nozomi Networks Labs[27]

2.4 Ransomware Tactics and Techniques

Referencing the MITRE ATT&CK framework, **a common technique that essentially defines the ransomware category within the "Impact" tactic**, is:

2.4.1 ID T1486 - Data Encrypted for Impact

The goal of implementing this specific strategy is to encrypt data on the target system, with the net effect of interrupting the regular workflow of its victims. Ransomware operators differentiate themselves based on the tactics used to extort payment, as well as the ability to compromise valuable targets.

When considering the "Initial Access" phase of the MITRE ATT&CK framework, we notice an evolution in ransomware deployments. In the past, threat actors relied heavily on spamming a consistent number of email addresses, hitting low value victims with high probability. In the last few months, ransomware operations have mostly switched to a more targeted model where high value victims are precisely selected and compromised.

Overall **the techniques used to gain an initial foothold within the target network** are:

2.4.2 ID: T1192 - Spearphishing Link

This technique involves sending an electronically delivered message to a target. It relies on social engineering to trick the victim into visiting a link, downloading a malicious file (an executable or a document) and clicking on the file. Alternatively, the malware attempts to exploit the target's browser or email reader.

2.4.3 ID: T1193 - Spearphishing Attachment

This technique involves sending an electronic message which includes an attachment, usually an executable or document, in the message itself. It relies on social engineering to trick the target into clicking on the attachment and initiating the attack.

2.4.4 ID: T1091 - Replication Through Removable Media

This technique relies on using removable media to transfer the malware, possibly leveraging the Autorun feature of the host operating system.

2.4.5 ID: T1190 - Exploit Public-Facing Application

This technique takes advantage of vulnerabilities in internet-exposed services. When a high-level vulnerability becomes public, ransomware operators rapidly scan valuable targets with the hope of finding an unpatched system. The public-facing application category includes both systems deployed on the organization's premises and systems hosted on cloud-based infrastructure.

2.4.6 ID: T1133 - External Remote Services

This technique relies on accessing a target network using services such as VPNs or Remote Desktop Protocols. Attackers rely either on credentials gained through brute force or harvested by other means, as well as on specific exploits. VPNs are often used by suppliers and contractors to perform their tasks. For this reason, supply chain and service organizations sometimes become a target and are exploited to ultimately attack their customers' systems.

2.4.7 ID: T1078 - Valid Accounts

Attackers harvest valid credentials for corporate accounts. For example, they use social engineering to obtain credentials that are reused on multiple services, or they buy stolen credentials from another threat group, then exploit the passwords.

MULTI-STAGE RANSOMWARE INFECTION

2. Threat Landscape

2.5 COVID-19-Themed Malware

While the techniques and methods for COVID-19-themed attacks we've observed are largely similar to the ones we normally see, the attackers now have an additional advantage. The climate of anxiety and uncertainty caused by COVID-19 makes the targets more susceptible to social engineering attacks.

Making matters worse, the number of companies adopting work-from-home policies to deal with the pandemic is tipping the scale in favor of the attackers. While some companies have infrastructure that allows remote work, such as VPNs and work laptops, others were not prepared and had to quickly come up with solutions, which might pose security risks.

COVID-19 has made remote work the new normal for everyone – including electric utilities and other critical infrastructure operators. In some cases, power utilities forced to send home hundreds of employees have **increased remote accessibility from just 9% of their machines to 53% in just a matter of days.**

Insurance Journal[28]

The COVID-19 pandemic has rapidly changed the social engineering focus of the threat landscape. One example is the warning issued by the World Health Organization (WHO) about phishing campaigns impersonating WHO officials.[29] These campaigns use email and social media channels in attempts to compromise readers by asking them to click on malicious links or open malicious attachments.

Targeting of healthcare institutions is also on the rise. For example, a research facility involved in performing medical trials on COVID-19 vaccines was recently hit by the Maze ransomware. Fortunately, the organization's computer systems were quickly restored without affecting operations or succumbing to the threat actor's demands. However, some patient information was exfiltrated and leaked online.

Cyber criminals have also begun selling COVID-19-themed phishing kits to those looking for easy ways to infect users. For example, attackers constructed a malware-infected replica of the Johns Hopkins University coronavirus tracking map to lure in victims.[30]

Various nation-states have also started using similar techniques to increase the effectiveness of their attack campaigns and advance their goals of stealing sensitive information and intellectual property.

> There's a risk of opening access to all of your plants. You're opening a new door that used to be closed. If it's an opening for you, it could be an opening for an attacker.
>
> ***Andrea Carcano, Co-founder and CPO, Nozomi Networks***

Online crimes reported to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) have roughly **quadrupled** since the coronavirus (COVID-19) pandemic.

MSSPAlert[31]

before the pandemic 1,000/day ▸ **since the pandemic** 4,000/day

2.6 COVID-19-Themed Tactics and Techniques

In 1H 2020 various phishing schemes attempted to lure users into giving up personal information or executing malicious software. Fake emails containing COVID-19 announcements from the WHO or other healthcare organizations were popular. Additionally, some emails pretended to inform the recipients about stimulus packages or pandemic-related shipping delays. Emails that impersonated the target's employer were also seen, containing letters of dismissal or instructions regarding work-from-home arrangements.

With respect to **the MITRE ATT&CK framework, COVID-19 is typically leveraged for the "Initial Impact" phase**, where the attacker tries to establish a presence within the target network. Further details are described below.

2.6.1 ID: T1193 - Spearphishing Attachment

This technique involves sending an electronically delivered message to a target. It relies on social engineering to trick the target into clicking on an attachment, which is an executable file or a document.

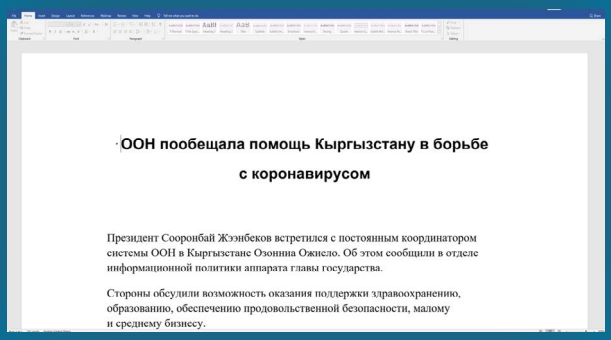
2.6.2 ID: T1192 - Spearphishing Link

This technique involves sending an electronically delivered message to a target. It relies on social engineering to trick the victim into visiting a link, downloading a malicious file (an executable or a document) and clicking on the file.

SPEARPHISHING EXAMPLE: CHINOXY BACKDOOR

Earlier this year, Nozomi Networks Labs analyzed **Chinoxy Backdoor**.

The .rtf file exploiting CVE-2017-11882 is embedded within a document containing information related to COVID-19 assistance, allegedly offered from the United Nations to Kyrgyzstan. The exploit is used to drop malicious binaries in the machine, which use HTTP over port 443 for C&C communication.



ООН пообещала помощь Кыргызстану в борьбе с коронавирусом

Президент Сооронбай Жээнбеков встретился с постоянным координатором системы ООН в Кыргызстане Озонния Ожисло. Об этом сообщили в отделе информационной политики аппарата главы государства.

Стороны обсудили возможность оказания поддержки здравоохранению, образованию, обеспечению продовольственной безопасности, малому и среднему бизнесу.

NOZOMI NETWORKS BLOG

COVID-19 Chinoxy Backdoor: A Network Perspective

To help the cybersecurity community defend its systems from COVID-19-themed threats, we monitored a prolific threat actor, very active in Asia, who has adapted malware delivery vectors to leverage the pandemic.

We've examined the Chinoxy Backdoor malware family, how it works and what tools can be used to detect it. We also provide a SNORT rule the security community can use to detect infections.

Nozomi Networks Labs[32]

NOZOMI NETWORKS LABS

COVID-19 Cybersecurity: Community Support

As the COVID-19 coronavirus has spread across the globe, malicious threat actors have found new ways to exploit the pandemic for their own gain. Critical infrastructure that we rely on for everyday life is being put at greater risk.

As a free service to the global security community, the Nozomi Networks Labs team is sharing its expertise by providing ongoing OT and IoT security support.

A multitude of resources are available on the Nozomi Networks COVID-19 Cybersecurity webpage: **nozominetworks.com/covid-19**

COVID-19 Threat Defense Training Sessions

Nozomi Networks Labs is hosting free COVID-19 Threat Defense training sessions for cybersecurity professionals and their teams.

COVID-19 OT and IoT Threat Intelligence

Nozomi Networks Labs is providing ongoing updates on COVID-19-related network indicators, ransomware and malware.

Guardian Community Edition

Nozomi Networks offers this free tool for OT and IoT security visibility. It includes specific checks for COVID-19-themed IOCs and remote access connections.

3. ICS Vulnerabilities

3.1 2020 Overview

Industrial Control Systems (ICS) typically include many devices, both legacy and new, that are insecure-by-design. Over the last 10 years, since the groundbreaking Stuxnet attack, industrial and OT networks have increasingly become the target of threat actors. Exploiting OT and IoT device vulnerabilities is a significant strategy for these attacks.

Vulnerabilities discovered in ICS systems provide attackers with opportunities to disrupt or manipulate data, which can impact physical processes and be extremely dangerous. It is therefore important to take the trends in vulnerabilities and weaknesses into account when evaluating security risks.

ICS-CERT,[33] a program run by a U.S. government body (CISA), publishes advisories on ICS vulnerabilities, exploits and security issues. It utilizes the Common Weakness Enumeration[34] (CWE) classification system for software and hardware vulnerabilities developed by MITRE.

Most organizations that deploy ICS software and hardware have increased their security awareness significantly over the last decade. For these asset owners, a reasonable course of action is to reduce exposure by first addressing the "low-hanging fruit," in terms of vulnerability discovery and patching. Over time, more and more vulnerabilities can be mitigated.

An example in the category of vulnerabilities requiring a relatively small effort to address, is Use of Hard-coded Credentials (CWE-798).

In comparison, mitigating Heap-based Buffer Overflow (CWE-122) or Stack-based Buffer Overflow (CWE-121) vulnerabilities is difficult. The fixes require firmware updates from vendors, the replacement of old equipment, or other mitigations. This group will likely continue to represent a significant percentage of the vulnerabilities discovered for the next few years.

Some of the most common flaws affecting ICS components during 1H 2020, based on advisories posted to ICS-CERT, are described below.

3.1.1 Buffer Overflows

Vulnerabilities caused by buffer overflows are one of the leading causes of weaknesses found in ICS software. Buffer overflows occur due a lack of bounds checking when data is written to a buffer, making it possible to corrupt adjacent data.

Attackers take advantage of this by creating denial of service states or executing their own code on vulnerable systems. There are ways to prevent or minimize the impact of buffer overflows, such as using memory-safe programming languages or exploit mitigations. However, in practice, ICS device vendors often face technical constraints, and do not address the issues.

3.1.2 Improper Access Controls

Improper access controls involve flaws in implementing authentication, authorization, or accountability control mechanisms. These flaws can result in threat actors accessing devices or systems with the privileges needed to read or steal information, or execute commands.

3.1.3 Improper Input Validation

Improper input validation problems occur when data input from external applications or devices is not properly filtered and corrected before it is recorded.

3.1.4 Uncontrolled Resource Consumption

Uncontrolled resource consumption involves implementation flaws stemming from improper handling of memory, storage or CPU resources. An attacker could remotely start an unlimited number of processes in a device. This could consume all the available memory and cause a denial of service condition.

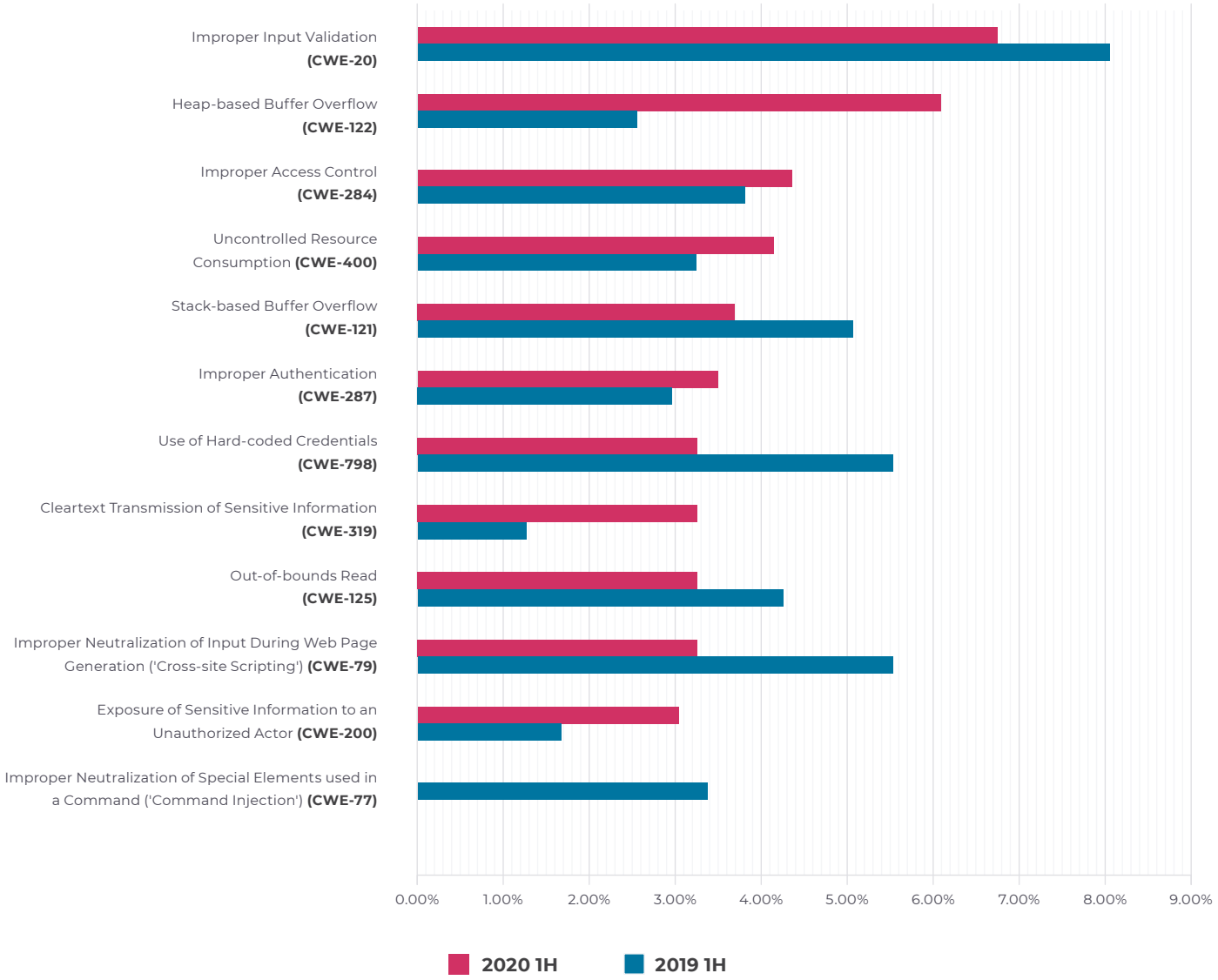
3.1.5 Cross-site Scripting

Cross-site scripting is a security vulnerability that allows attackers to inject malicious payloads into trusted content. Subsequently, innocent users access and load the content, initiating the attack.

ICS VULNERABILITIES REMAIN A CHALLENGE

VULNERABILITY TYPE	MITIGATION DIFFICULTY
Improper Input Validation (CWE-20) The top type of disclosed vulnerability from 2019 to 2020.	Low
Buffer Overflows (CWE-120, CWE-122) **Uncontrolled Resource Consumption (CWE-400)** Two of the top five vulnerability types disclosed from 2019 to 2020.	High

3.2 Common Vulnerability Types



OUTLOOK

Difficult-to-mitigate vulnerabilities will be a significant category of risk for the next few years.

RECOMMENDATIONS

Asset owners should take a **multi-pronged approach** of monitoring, vulnerability elimination and vulnerability mitigation.

4. Recommendations

4.1 OT/IoT Network Visibility and Monitoring is Key

Monitoring and improving the security posture of a network is a continuous process for any blue team. Rapidly evolving threats constantly challenge defenders to deploy effective countermeasures to keep users safe. To avoid being outpaced by the sheer number of attacks, it is paramount to have a detailed understanding of common threat characteristics and be ready to implement specific defensive strategies.

4.1.1 IoT Malware

The security of IoT devices is a problem that will continue to grow as more connected devices reach the market and are deployed into networks. While these devices help streamline operations, they also attract new attack vectors.

For instance, the attack surface available to IoT malware for threat propagation is often related to services that should not be exposed to the internet. Before deploying a new IoT device, a proper assessment should be performed to understand whether or not the network exposure it creates is strictly limited to that required for device operation. Whenever possible, IoT device services should not be exposed to the public internet.

Supply chain attacks are extremely difficult to detect, and this reality is even more true in the context of IoT. Most of the time when an organization deploys an IoT device, there's very little visibility into the firmware running on it. Organizations simply accept the fact that the device is a black box. Complete network visibility and monitoring is needed to protect your organization from a supply chain attack that hits an IoT device.

It is possible to monitor IoT devices over time with an OT/IoT network visibility solution. For instance, consider the case where a firmware update has supply chain attack code. A real-time threat detection and monitoring solution would pinpoint the moment the device begins exhibiting malicious behavior, correlate the event with the update, and generate urgent alerts. Action can be immediately taken to block or mitigate the attack.

4.1.2 Ransomware

In the last few months, we have seen ransomware operators changing tactics to maximize the impact of their attacks. As more and more organizations put proper backup and disaster recovery procedures in place, ransomware crews adapted by stealing and then threatening to leak sensitive company data. To mitigate this new risk factor, organizations should carefully segment and properly authorize access to internal data, and periodically review such policies.

During the first half of 2020 we saw the first ransomware targeting industrial automation software (SNAKE/EKANS) that moved laterally within the victim network to search for valuable data to encrypt and/or steal. To properly defend an OT/IoT network from this kind of intrusion, it is necessary to use a network monitoring solution to detect and stop the intrusion while it is still in the reconnaissance phase.

4.1.3 COVID-19-Themed Malware

Phishing is an ongoing threat that constantly adapts to changes in the technological and socio-economic environment, such as the widespread work-from-home policy adopted during the COVID-19 emergency.

In general, phishing mitigations can be divided into two macro categories.

The first one relates to general awareness and education for people commonly targeted by phishing attacks. Investing in employee training and conducting internal exercises can help an organization understand its phishing security posture. It also helps identify the technical countermeasures that could be deployed. This is even more urgent today, as a significant portion of the workforce has moved from using protected office networks to less secure home and public networks.

The second mitigation tactic involves isolating the specific phishing vectors recently used by attackers, and neutralizing each one of them. For instance, with phishing attacks that rely on malicious documents to deploy malware, a viable strategy would be to move the company to SaaS-based services for business applications and documents.

If you need to better protect your organization from credential theft, an optimal solution would be to use a centralized identity provider with multi-factor authentication.

4.1.4 ICS Vulnerabilities

Asset stakeholders are advised to implement processes that ensure the continuous monitoring of systems and the vulnerabilities affecting them, and to use tools for asset visibility.

Vulnerability knowledge should be paired with anomaly detection and up-to-date threat signatures. Threat signatures identify known Indicators of Compromise (IoCs) while anomaly detection identifies unusual behavior that could indicate that an advanced attacker is using a vulnerability that has not yet been made public.

4.2 Summary of Actionable Recommendations

Threat or Risk	Recommendations
IoT Malware	Avoid exposing IoT devices to the public internet when possible. Thoroughly assess the security posture of devices and implement proper monitoring when internet exposure is required.
	Limit the services exposed for any IoT device to those strictly required for core functionality, even when the device is used on internal networks.
	Verify with the vendor that any undocumented remote access mechanism is removed from production firmware.
	Change the factory-set credentials for devices with documented remote access capabilities, or, if possible, disable the functionality.
Ransomware	Compartmentalize corporate data according to its strategic importance and implement a matching escalating scale of defensive policies.
	Review your network monitoring policies and test/improve the reaction time for security events.
	Assess your attack surface carefully and whenever possible, apply patches as soon as they become available, and implement proper network and device monitoring.
COVID-19-Themed Malware	Review your company's defensive strategies for spearphishing attacks.
	Perform simulated attacks against your remote workforce to understand your real security posture. This is especially important in the new work-from-home environment.
	Phishing attack mitigation should fit into the global activities performed by teams responsible for operational security.
ICS Vulnerabilities	Monitor your systems for vulnerabilities and act on the ones that pose the most risk to your organization.
	Use OT/IoT threat and anomaly detection technologies to speed response and mitigation times.

5. Conclusion

Shifting OT/IoT Threats Require High Cyber Resiliency

This report documents the threats to OT and IoT networks that occurred in the first half of 2020. We expect that attacks from IoT botnets, ransomware and COVID-19-themed malware will continue to grow, though they will shift and adapt in the second half of the year.

ATTACKERS SHIFT THEIR SIGHTS TO OT

Threat actors continue to shift their sights to different attack vectors, with **increased targeting of IoT devices, Operational Technology (OT), and connected industrial and medical systems.**

IBM Security[2]

Given that threats are increasing and constantly changing, it's important to maintain high cyber resiliency and fast response capabilities. In this regard, security gaps related to people, processes and technology have a large impact. For example, the separation of IT and OT in organizations with increasingly connected IT, OT, and IoT systems, can lead to blind spots. But, with the right technology and a focus on best practices, you can increase visibility and operational resiliency.

We encourage you to subscribe to Nozomi Networks Labs and utilize our cybersecurity community resources[35] to stay on top of the latest threats.

In addition, the Nozomi Networks solution significantly advances OT/IoT visibility and cybersecurity. It delivers visibility by automatically and safely creating an up-to-date inventory and visualization of all assets on the network. It then monitors behavior for anomalies and threats, and alerts operators to changes that could indicate critical incidents.

The solution delivers ongoing OT and IoT threat and vulnerability intelligence for rapid risk reductions. And, with continuous OT and IoT asset intelligence it eliminates anomaly alert overload.

Especially in environments with high numbers of devices that generate many anomalies, it is essential to focus your attention on critical incidents and keep the mean-time-to-respond short. Insights provided by the Nozomi Networks solution will help you do just that.

FIND OUT MORE

The world's top global industry leaders have chosen our innovative solution for OT and IoT visibility and threat intelligence. It significantly helps them accelerate digital transformation and reduce cyber risk.

Find out how quickly the Nozomi Networks solution can boost operational resiliency for you.

Contact us at **nozominetworks.com/contact**

> The steep rise in the number of threats targeting and/or impacting operational networks should be a serious concern for IT security professionals responsible for keeping not only IT, but OT and IoT networks safe.
>
> Today, as IT, OT and IoT worlds converge, threat actors of all types are increasingly setting their sights on higher value targets, often critical infrastructure organizations.
>
> Defending OT and IoT networks is a daunting task, but not impossible. We know from working with thousands of industrial installations that you can monitor and mitigate these risks, whether they stem from cybercriminals, employees or nation-states.
>
> **Andrea Carcano, Co-founder and CPO, Nozomi Networks**

6. References

1. **"IoT – The Internet of Transformation 2020,"** Juniper Research, April 2020.
2. **"X-Force Threat Intelligence Index 2020,"** IBM Security, February 2020.
3. **"An Updated Assessment of the Economic Impact of COVID-19,"** Asian Development Bank, May 2020.
4. **"Protecting Businesses Against Cyber Threats During COVID-19 and Beyond,"** Google, April 2020.
5. **"Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020,"** Gartner, August 2019.
6. **"2020 Unit 42 IoT Threat Report,"** Palo Alto Networks, March 2020.
7. **"Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis,"** Cloudflare, December 2017.
8. **"New dark_nexus IoT Botnet Puts Others to Shame,"** Bitdefender, April 2020.
9. **"Dark Nexus IoT Botnet: Analyzing and Detecting its Network Activity,"** Nozomi Networks, May 2020.
10. **"New Mirai Variant Targets Zyxel Network-Attached Storage Device,"** Palo Alto Networks, March 2020.
11. **"CVE-2020-9054 Detail,"** National Vulnerability Database, March 2020.
12. **"The LeetHozer Botnet,"** Netlab 360, April 2020.
13. **"Mirai and Hoaxcalls Botnets Target Legacy Symantec Web Gateways,"** Palo Alto Networks, May 2020.
14. **"Grandstream and DrayTek Devices Exploited to Power New Hoaxcalls DDoS Botnet,"** Palo Alto Networks, April 2020.
15. **"Mozi, Another Botnet Using DHT,"** Netlab 360, December 2019.
16. **"New Mozi Malware Family Quietly Amasses IoT Botnets,"** CenturyLink, April 2020.
17. **"MITRE ATT&CK,"** MITRE.
18. **"Digital Assets and Data Management – Managing Enterprise Risks and Leveraging Data in a Digital World,"** BakerHostetler, April 2020.
19. **"Navigating the MAZE: Tactics, Techniques, Procedures Associated with MAZE Ransomware Incidents,"** FireEye, May 2020.
20. **"Cyber Gangsters Hit UK Medical Firm Poised for Work on Coronavirus with Maze Ransomware Attack,"** ComputerWeekly, March 2020.
21. **"Ransomware Gangs to Stop Attacking Health Orgs During Pandemic,"** BleepingComputer, March 2020.
22. **"Hackers Cripple Airport Currency Exchanges, Seeking $6 Million Ransom,"** The New York Times, January 2020.
23. **"REvil Ransomware Creates eBay-like Auction Site for Stolen Data,"** BleepingComputer, June 2020.
24. **"Another Hacked Florida City Pays Ransom, This Time for $460,000,"** The New York Times, June 2019.
25. **"DoppelPaymer Ransomware launches Site to Post Victim's Data,"** BleepingComputer, February 2020.
26. **"Mexico's Pemex Oil Suffers Ransomware Attack, $4.9 Million Demanded,"** BleepingComputer, November 2019.
27. **"Snake Ransomware is Raising Concerns for Industrial Control Systems,"** Nozomi Networks, February 2020.
28. **"Employers Beware: Working from Home Creates New Cyber Risks,"** Insurance Journal, March 2020.
29. **"Beware of Criminals Pretending to be WHO,"** World Health Organization.
30. **"John Hopkins University Statement on Malware Disguised as COVID-19 Map,"** John Hopkins University, March 2020.
31. **"FBI: Covid-19 Cyberattacks Spike 400% in Pandemic,"** MSSPAlert, April 2020.
32. **"COVID-19 Chinoxy Backdoor: A Network Perspective,"** Nozomi Networks, April 2020.
33. **"ICS-CERT Advisories,"** Department of Homeland Security.
34. **"Common Weakness Enumeration,"** MITRE.
35. **"Nozomi Networks Labs: COVID-19 Cybersecurity: Community Support,"** Nozomi Networks.

NOZOMI NETWORKS

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

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.

NN-SEC-RP-2020-IH-8.5X11-001

nozominetworks.com