NOZOMI NETWORKS

LABS

RESEARCH REPORT

OT/IoT Security Report

Supply Chain and Persistent Ransomware Attacks Reach New Heights

February 2021

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

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. Throughout the body of the text, words in blue take you to a location with additional information on the topic.

1. Executive Summary

As society deals with the second year of the COVID-19 pandemic, organizations are accelerating digitization to survive and thrive. This places more focus on operational systems, which are at the heart of value and revenue creation.

Adding to challenges, cybersecurity is ranked by executives as the second highest risk to enterprises,[1] and attacks on critical infrastructure are rated as the fifth highest global risk by the World Economic Forum.[2]

To help security teams and operators of OT and IoT environments, this report provides an overview of the most significant threats and vulnerability trends of recent months. It also provides actionable insights and recommendations for securing operational systems.

We encourage organizations to focus on security fundamentals and to assess their security posture against the threats and vulnerabilities described in this report for enhanced operational resilience.

In surveying the threat landscape since we published our report on the first half of 2020, two types of threats stand out: supply chain and persistent ransomware.

Supply Chain Threats and Vulnerabilities

The most notable cyber operation of 2020 is the SolarWinds supply chain attack that resulted in the infection of thousands of organizations. This attack, plus recent vulnerability trends, mean that now is the time for asset owners to reevaluate the attack surfaces of their OT/IoT systems, and reassess supply chain risks.

The SolarWinds attack involves an advanced threat actor that compromised a SolarWinds network monitoring product widely used to manage IT infrastructure.

Victims of the attack include U.S. government agencies plus critical infrastructure and manufacturing operations. The damage is sophisticated espionage, with unknown impacts in the future.

The SolarWinds supply chain attack is the most notable threat of 2020.

In terms of scope and sophistication it is one of the most successful espionage operations ever discovered.

Although the SolarWinds threat actor carefully selected just a few targets to receive the malicious payload that allows them to have further access within compromised networks, all infected organizations now face the significant challenge of sanitizing their networks.

The SolarWinds attack also reflects the most important recent vulnerability trend, which is supply chain research and exploitation. It is an example of a threat actor very carefully selecting a widely used service or software as its supply chain target. This attack highlights the risks to end users who have limited agency over the software used within their networks.

Another type of software supply chain threat is embedded component risk, as exemplified by the Ripple20 vulnerabilities.

Ripple20 consists of 19 vulnerabilities identified in the TCP/IP stack from Treck.

At the time of exposure there was high concern about the risks these vulnerabilities posed to IoT devices. However, later in the year, additional research showed that there is little chance that many targets meet the requirements needed for exploitation by a motivated actor.

Attack surface reduction and network segmentation are two best practices to counter supply chain risks. In addition, OT and IoT network monitoring is a key technology that helps define the attack surface and detect anomalous activity indicative of an advanced threat.

Ransomware

Ransomware threat actors dominate the threat landscape, doggedly targeting organizations they believe can pay lucrative ransoms. And, they are not just demanding financial payments, but are exfiltrating data and deeply compromising networks for future nefarious activities. Sadly, targets include healthcare organizations researching and producing vaccines for COVID-19.

The sophistication of ransomware criminals is increasing, as more are using combinations of strategies and threat vectors. A prime example is the Ryuk ransomware group, which is estimated to be behind a significant percentage of all ransomware attacks in 2020.[3]

Ryuk's cyber kill chain includes:

- Phishing email
- BazaarLoader execution
- Cobalt Strike deployment
- Domain discovery
- ZeroLogon against DC (domain controller)
- Additional asset discovery
- Ransomware deployment

Amazingly, depending on the targeted network, the length of time from initial infection to ransomware execution can be as fast as a couple of hours.

Examples of best practices to counter ransomware are identity and access management and disaster recovery planning.

Ransomware is the second most notable threat category.

These attacks continue to grow in frequency and significance, utilizing an expanded toolset and deeply compromising victim networks for maximum impact.

Other Notable Threats

In terms of other notable threats, social engineering attacks are ongoing. For example, in the second half of 2020, threat actors used society's widespread interest in COVID-19, Black Lives Matter and the U.S. presidential election to deceive victims into executing malicious software or leaking credentials. Typically the content of social engineering attacks is tied to news cycles and this fact should be highlighted in end user cybersecurity training programs.

Both nation state and ransomware threat groups are targeting healthcare, specifically COVID-19 research organizations. They are also using off-the-shelf red team tools to effectively execute attacks.

This report includes information on 18 specific threats that IT and OT security teams should study as they model threat vectors and evaluate risks across operational technology systems.

IoT IS AN EASY AND PLENTIFUL TARGET FOR ATTACKERS

98% of all IoT device traffic is unencrypted

57% of IoT devices are vulnerable to medium or high severity attacks[4]

Vulnerability Trends

We analyzed 151 industrial advisories published by ICS-CERT and classified them into CWE categories.

Memory corruption errors are the dominant type of vulnerability for industrial devices. We expect this situation to continue as many ICS assets lack intrinsic security and receive limited security oversight.

In a threat landscape where ransomware organizations are attacking companies indiscriminately, it's vital to understand the vulnerabilities under active exploitation. This risk is heightened by the fact that nation state groups are utilizing non-zero-day vulnerabilities to conduct sophisticated attacks.

Organizations should focus on identifying unpatched software and implementing update or mitigation policies. Subscription to threat intelligence services helps by providing current OT and IoT threat and vulnerability intelligence.

IoT Security Guidelines

Organizations and technology vendors must now deal with increasing government oversight when dealing with IoT cybersecurity.

For example, the U.S. passed the IoT Cybersecurity Improvement Act, a first step towards mandating baseline security practices for IoT devices. Similarly, the E.U. has published Guidelines for Securing the IoT, specifically focusing on the supply chain of IoT assets.[5]

Recommendations

Simply knowing attack and vulnerability numbers for a given timeframe is not the way to assess risk. It provides a skewed representation of the actual risks faced by an organization.

Instead, security teams should continuously improve security fundamentals, and assess how these measures behave against the major emerging threats.

To help defenders with the current threat landscape, this report includes actional insights in the following areas:

- Network Monitoring
- Attack Surface Reduction
- Network Segmentation
- Identity and Access Management
- Disaster Recovery Planning
- Active Directory Hardening
- Secure Remote Access
- DNS over HTTPS
- Detection of Blockchain-based Infrastructure
- Awareness of Legitimate Online Service Abuse

These topics cover both general-purpose suggestions for improving cyber resilience as well as niche measures that address recent threats.

Moving onward from 2020, a year of unprecedented change, a few things are clear. Operational technology and critical infrastructure systems are more important than ever to healthcare, economies, and societies.

As cyber threats evolve and increase, understanding the effectiveness of defenses against the emerging threat and vulnerability landscape is vital.

10 ACTIONABLE INSIGHTS

Network Monitoring

Attack Surface Reduction

Network Segmentation

Identity and Access Management

Disaster Recovery Planning

Active Directory Hardening

Secure Remote Access

DNS over HTTPS

Detection of Blockchain-based Infrastructure

Awareness of Legitimate Online Service Abuse

By providing current threat and vulnerability analysis, along with recommendations, this report aims to help organizations assess and enhance their security posture.

Companies that move forward with improving OT/IoT visibility, security, and threat intelligence are best able to ensure the availability, safety and confidentiality of their operational systems.

1

Threat Landscape

2.1 Introduction

To protect your critical networks and the intellectual property related to them, you need current information about the threat landscape and the regulatory environment related to it.

Understanding the SolarWinds attack is essential, not just for SolarWinds customers, but for all organizations as you evaluate your exposure to supply chain attacks. Ransomware attacks are also important. They are increasing in frequency and threaten not just financial resources, but long-term network compromise and possible compliance challenges. Social engineering techniques continue to flourish, taking advantage of trending topics, such as COVID-19, Black Lives Matter and the 2020 U.S. presidential elections.

IoT devices are proliferating in operational environments and are typically insecure-by-design. New regulations are coming into place in the E.U. and the U.S. to improve their intrinsic security and help you with best practices for deployment.

Related to the pandemic, healthcare organizations are under high attack pressure both from ransomware and threat actors conducting cyber espionage. If you are in this industry you should treat network compromises with the utmost priority.

2.1.1 SolarWinds

There are a few distinguishing characteristics that set high-profile nation states threat actors apart from regular cybercriminal syndicates. One of the most defining is their ability to deeply analyze the supply chain structure of potential targets.

This was disturbingly well done with the selection of **SolarWinds**, the developer of a network management software. Among its users are multiple U.S. government agencies and many strategically important private companies. From the perspective of a resourceful attacker, SolarWinds software checks all the boxes in terms of its end users and the privileged access that its software has within an organization's network.

The supply chain attack carried out through the SolarWinds breach is the most significant threat campaign of 2020.

An **overview of the attack** is presented later in this report. The espionage operation started as far back as August 2019 and only began to unravel in December 2020, with the disclosure of a sophisticated breach by the security company FireEye. While the total number of affected organizations is in the thousands, only a few carefully selected targets are known to have received the malicious payload that allows the attackers to have further access within compromised networks.

The full impact of the SolarWinds malware campaign is not yet publicly known. More information continues to be uncovered, and we will have more analysis of this attack in future reports. Unfortunately, with an attack of this complexity, there is no single technical defense. Instead, every organization should be looking to continuously improve its security posture and processes.

2.1.2 Ransomware

Ransomware operations continue to be particularly active, indiscriminately hitting valuable companies that might be extorted for financial gain. These threats have traditionally been labelled as “ransom” because of the monetization strategy employed. However, strategically, the risk they pose is much higher than solely financial.

Today’s ransomware threat actors constantly adjust their toolsets and have mastered the skills required to gain an initial foothold in a targeted network and then deeply compromise it. This allows them to steal confidential information and maintain an ongoing presence for future harm.

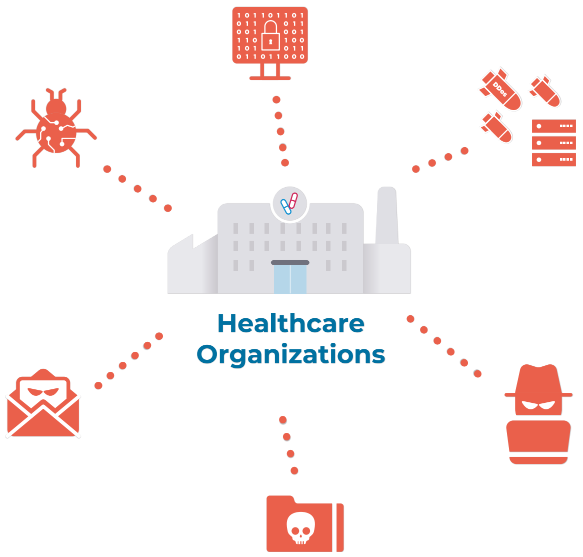
In terms of intellectual property, the threat of losing highly coveted trade secrets might disproportionally impact industries heavily based on research, while others could be relatively immune. Even in the latter case, however, the risk of strategic contracts landing in the hands of a competitor justifies taking ransomware threat groups very seriously.

Once a malicious actor has been observed repeatedly exhibiting this capability, there are several considerations for defenders. Security teams responsible for defending networks should verify their posture against known ransomware TTPs (Tactics, Techniques and Procedures). Carefully studying the details of recent incidents, most notably the Norsk Hydro attack of 2019, can help organizations understand potential consequences and prepare actionable contingency plans.

At the strategic level, defenders should assess the potential harms of network compromise. For example, if your company plays a key role in a specific supply chain, compromise could have consequences for society. Microsoft acknowledged the danger of this type of situation in October. They executed a carefully planned takedown of several key elements of the infrastructure used by Trickbot, a botnet known for providing services to both nation states and criminal groups.[6]

Handling a ransomware compromise also has regulatory implications that vary between countries. For example, late last year the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) issued an advisory to organizations willing to pay ransom requests. They warned that, according to their guidelines, if the malicious actor receiving the payment is among a list of individuals sanctioned by OFAC, the paying party will be liable of violating U.S. sanctions.[7]

In the E.U., the General Data Protection Regulation dictates a series of actions that must be completed in the aftermath of a data breach.[8] There are serious economic consequences to organizations if there is a violation of these rules. Therefore, regulatory compliance is another complex impact of a ransomware attack that requires careful and advanced planning to avoid a crisis.



To the disbelief of many, particularly given the ongoing COVID-19 pandemic, **healthcare** is still one of the sectors highly targeted by ransomware, as described later in the report. Organizations directly involved in researching and producing vaccines and cures for COVID-19 have found themselves at the center of attacks.

2.1.3 Nation State Threats

Notable nation state attacks targeting the **U.S. presidential election** and **healthcare** organizations doing COVID-19 research are discussed later, in sections devoted to those topics.

On other fronts, in October, the NSA released an advisory listing a series of public vulnerabilities that were actively being exploited by Chinese nation state actors.[9]

This publication is particularly important to industry for several reasons:

- First, an entity with broad visibility of the threat landscape, that is, the NSA, provided fascinating insight into the tradecraft used by another nation state against difficult targets.
- Second, it highlights how patching is still an unsolved problem for many organizations.
- Third, it provides a specific list of vulnerabilities that is completely actionable for any security team.
- Finally, the details provided in the advisory go a long way towards helping organizations keep networks safe and ensuring business continuity.

2.1.4 IoT Security

In November the U.S. Congress passed the IoT Cybersecurity Improvement Act,[10] an important first step towards mandating baseline security practices for the development and deployment of IoT devices.

The bill specifically assigns NIST with the task of issuing guidelines and recommendations for the appropriate use and management of IoT devices owned or controlled by the government. NIST, along with the Office of Management and Budget, is to provide guidance on the disclosure process of security vulnerabilities affecting IoT devices.

ENISA, the European Union Agency for Cybersecurity, has also released a new publication on IoT security, called Guidelines for Securing the IoT, specifically focused on providing actionable recommendations for the supply chain of IoT.[11]

NOZOMI NETWORKS BLOG

The U.S. Government is Creating Security Standards for IoT Devices

The lack of security standards for IoT devices has been an issue since they became popular a decade ago. Their widespread usage has outpaced industry's ability to agree on how to protect them.

This changed in 2020 when a customer with deep pockets, the U.S. government, legislated the development of baseline security practices in four areas:

- Secure development
- Identity management
- Patching
- Configuration management

The U.S. Internet of Things Cybersecurity Improvement Act of 2020 was signed into law on December 4, 2020.[12]

2.1.5 Pandemic-Related Targets

Healthcare organizations have clearly been stressed in recent months from the day-to-day tasks of handling COVID-19 outbreaks. In the cyber realm, healthcare entities face two categories of threat actors. First, ransomware crews trying to disrupt operations during the pandemic, and second, nation state actors performing cyber espionage targeting facilities involved with COVID-19 research.[13]

In terms of ransomware attacks, CISA, the FBI, and the HHS* released an alert about an imminent threat to U.S. hospitals and healthcare providers in October.[14] The alert describes an infection chain that starts with **Trickbot/Bazar** and ends with deployment of the **Ryuk** ransomware. What stands out about this alert is the amount of actionable information provided, both in terms of IoCs and general-purpose mitigations for security teams.

The next month, a hospital in Düsseldorf, Germany, was forced to cut the number of admissible patients by half after its network infrastructure was compromised by DoppelPaymer ransomware. The outcome was tragic – one person with a time sensitive condition died after their ambulance was redirected to a hospital much further away. A prosecutor in Cologne tried to charge the attackers with the death.[15] Although the investigation concluded that there were insufficient grounds to open a formal case, this episode is a sad statement of the possible physical consequences of a ransomware attack.

Regarding nation state attacks, Microsoft publicly announced that it has been at the forefront of detection and response to attacks originating from three different nation state actors. The attacks were against leading pharmaceutical companies and vaccine researchers in Canada, France, India, South Korea and the United States.[16]

In a variation on nation state attacks, the U.S. Justice Department charged two Chinese men with cyber espionage targeting intellectual property related to COVID-19 research.[17] The most interesting aspect of this indictment is that prosecutors identify the men as “private hackers” working with occasional support from Chinese Ministry of State Security (MSS). This is further evidence of an ongoing trend where some private cybercrime groups are behaving, at least partially, as loosely coupled elements of government agencies. The line is often blurred between activities attributable to regular crime and those with broader impact, such as industrial espionage.

In December, IBM Security X-Force made public a broad spearphishing campaign targeting several private and public organizations in Germany, Italy, South Korea, Czech Republic, Europe and Taiwan.[18] The targets were all apparently involved with the ongoing effort to distribute the first COVID-19 vaccines, which notoriously require extremely low temperatures to store. The scope of the victims and the background information required to craft the spearphishing messages suggests that a nation state actor might be behind this campaign, but the evidence is not definitive.

Given the ambiguity and the complexity of this hybrid landscape, healthcare entities should treat network compromises with the utmost priority, comparable to healthcare emergencies.

** The U.S. Cybersecurity and Critical Infrastructure Security Agency, the U.S. Federal Bureau of Investigation, and the U.S. Department of Health and Human Services.*

2.1.6 2020 U.S. Presidential Election

The buildup to the U.S. presidential election was of high interest to many around the world and threat actors were no exception. They used topics related to the election in phishing emails to gain access to systems for purposes such as ransom (**Emotet**). And, U.S government authorities identified malicious actors and nation states attempting to influence political campaigns and the voting process.

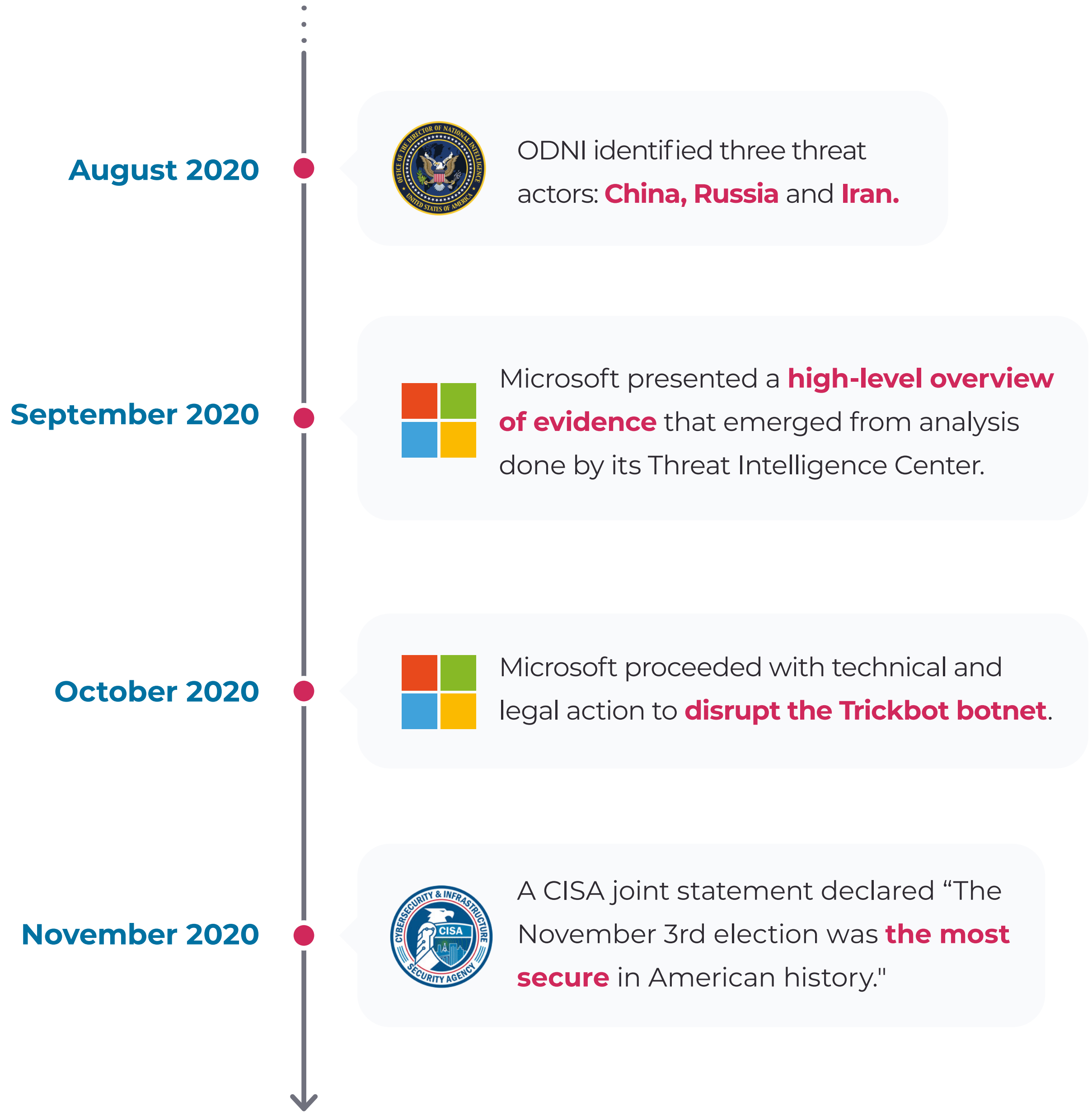
For example, as early as August, the Office of the Director of National Intelligence (ODNI) identified three different threat actors whose ongoing and potential activity was deemed concerning: China, Russia and Iran.[19] In the following months, evidence of attacks against organizations involved in the political campaign emerged, substantiating ODNI's early warning.

To counter the threats, CISA ran a comprehensive cybersecurity initiative called #PROTECT2020.[20] In practical terms it meant not only securing the actual casting and counting of the ballots, but also monitoring political campaigns. It was important to defend against all attacks by malicious actors that wanted to influence the outcome of the democratic process.

Private companies also contributed. In September, Microsoft presented a high-level overview of evidence that emerged from analysis done by its Threat Intelligence Center (MSTIC). Three actors related to the nation states identified by ODNI were recognized as those most actively attacking organizations directly involved in U.S. political campaigns. (A single group was also found to be targeting European political organizations, as well as think tanks with specific interests in European policies.)

In October, Microsoft proceeded with technical and legal action to disrupt the **Trickbot** botnet. They feared that a nation state actor could leverage criminal groups' access to critical systems, with the goal of disseminating chaos and distrust in the electoral process.[21]

The result of bold action by both the U.S. government and the private sector was reflected in a CISA joint statement declaring: "The November 3rd election was the most secure in American history."[22]



August 2020

ODNI identified three threat actors: **China, Russia** and **Iran.**

September 2020

Microsoft presented a **high-level overview of evidence** that emerged from analysis done by its Threat Intelligence Center.

October 2020

Microsoft proceeded with technical and legal action to **disrupt the Trickbot botnet**.

November 2020

A CISA joint statement declared "The November 3rd election was **the most secure** in American history."

2.1.7 Social Engineering

Leveraging social events to deceive victims into executing malicious software or leaking valid credentials is a classic tool in an attacker's playbook.

To tackle this issue at a strategic level, we can break this phenomenon down in two dimensions. The first consists of understanding the vectors used to deliver the content, such as emails, social media or malicious advertising. We can be more granular, for example contrasting regular spam versus business email compromise. However, this part of the problem tends to be more static in nature and, as a consequence, well understood.

The second dimension is the content presented to the victim – this aspect inherently exhibits more variation. It is typically tied to news cycles and is sometimes localized to specific geographic or cultural regions.

In the second half of 2020, the most-used topics for social engineering were COVID-19, the Black Lives Matter movement, and the 2020 U.S. presidential elections.[23]

COVID-19 has been the theme overwhelmingly leveraged to deliver malicious payloads of any type. In the second half of 2020 this trend shifted to more refined messaging that touched on the day-to-day realities imposed by the pandemic, such as late shipping notices or government relief applications. A further unique threat has been the distribution of links to fake contact tracing applications.

Black Lives Matter, a movement advocating for racial justice, has been used by spammers to distribute Trickbot.

The U.S. 2020 presidential election was utilized by malicious actors to lure potential victims. The most notable example was an October 2020 spam campaign by the threat group behind the Emotet malware. The email messages contained a fake call to action from the Democratic National Committee, including a Word document that triggered an infection chain when it was clicked.

2.2 The MITRE ATT&CK® Framework

ATT&CK®

The MITRE ATT&CK® Framework provides a map of tactics and techniques commonly used by adversaries.[24] The techniques it documents are used to understand complex attack scenarios, providing actionable insight to defenders. Furthermore, the framework provides a common language which is used by the security community to analyze and effectively communicate about incidents. Having a common reference point can be useful in enhancing an organization's security strategies and policies.

The "ATT&CK for ICS" framework is a complementary knowledgebase to "ATT&CK for Enterprise" and aims to describe incidents involving ICS (Industrial Control System) networks, which are outside the latter's scope.

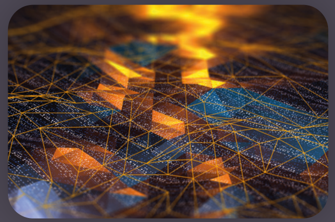
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Model	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

[24] *https://collaborate.mitre.org/attackics/index.php/Main_Page*

In the material that follows, we include references to various MITRE ATT&CK framework techniques when we describe malicious software or threat actors. Comprehensively describing every single technique used by a specific malicious sample, or over the lifetime of a malicious actor, is out of scope for this report. Thus, the MITRE references are starting points for security teams aiming to gain a deeper understanding of the relevant tactics and techniques.

In the cases where a technique is represented by both the Enterprise matrix and the ICS matrix, we have cited both technique IDs. While the framework is maturing and evolving, security incidents can cross the theoretical dividing lines between IT, OT and IoT in a network. It is therefore important to keep in mind that the two knowledgebases are, in some cases, best used together.

NOZOMI NETWORKS BLOG



Your Guide to the MITRE ATT&CK Framework for ICS

The MITRE ATT&CK® Framework for Industrial Control Systems (ICS) threat modeling classifies malicious cybersecurity events against an operational technology (OT) environment.

This article introduces you to:

- The MITRE ATT&CK framework ontology
- The differences between the MITRE ATT&CK frameworks for IT and ICS
- The MITRE ATT&CK framework for ICS implementation

We believe that the MITRE ATT&CK Framework for ICS is effective in describing incidents and providing detailed insight into threat actors' behavior. It can be used by security teams to enhance security strategies and policies.[25]

3

Notable Threats

3.1 Synopsis of 18 Threats

3.1.1 FireEye Compromise

In December, security company FireEye publicly reported that its network was successfully compromised by a sophisticated nation state actor. The targeted attack managed to exfiltrate custom red team tools used by FireEye to assess the security posture of its customers. The company rushed to provide publicly available IOCs to help organizations defend against attacks leveraging the tools.

FireEye conducted a thorough investigation into the root cause of initial access and realized that their company was just one of many organizations breached. Access was provided through Orion, a network monitoring product developed by the company SolarWinds, which is widely used to manage IT infrastructure.

Given the high-profile impact of the discovery, the details were revealed to the public quickly, only a few days later.[26]

3.1.2 SolarWinds (SUNSPOT, SUNBURST, SUPERNOVA)

FireEye later published a blog post revealing the details of the attack. It was a supply chain attack, where a SolarWinds Orion software update was hijacked to distribute malware to thousands of organizations.

Additionally, a CISA Computer Emergency Readiness Team (CERT) Emergency Directive (Emergency Directive 21-01) was published the same day.[27] It provided background information and suggested actions for infected parties.

Based on the current state of the incident's investigation, evidence points to the threat actor having access to SolarWinds infrastructure as far back as September 2019. According to SolarWinds, the October 2019 release of the Orion Platform contained modifications indicating the threat actor was likely testing their ability to inject code into the product during the build process.[28]

CrowdStrike's analysis of SUNSPOT, the malware used to inject SUNBURST into builds of SolarWinds' Orion, suggests that build processes were monitored so that the target source file could be replaced with a modified one.[29] What is remarkable is the apparent attention to detail displayed. Specifically, the threat actor took measures to avoid triggering any crashes or anomalies during the compilation process, avoiding alerting SolarWinds' developers of a problem.

The SUNBURST backdoor was deployed in the February 2020 Orion Platform release.

Based on an SEC filing by SolarWinds, "fewer than 18,000" customers received the malicious digitally signed update.[30] SUNBURST stays dormant for up to two weeks after its deployment and then contacts C&C (Command and Control) to receive further instructions. The communication with C&C relied on a network protocol used by Orion, and was stored inside legitimate plugin files, making detection challenging.

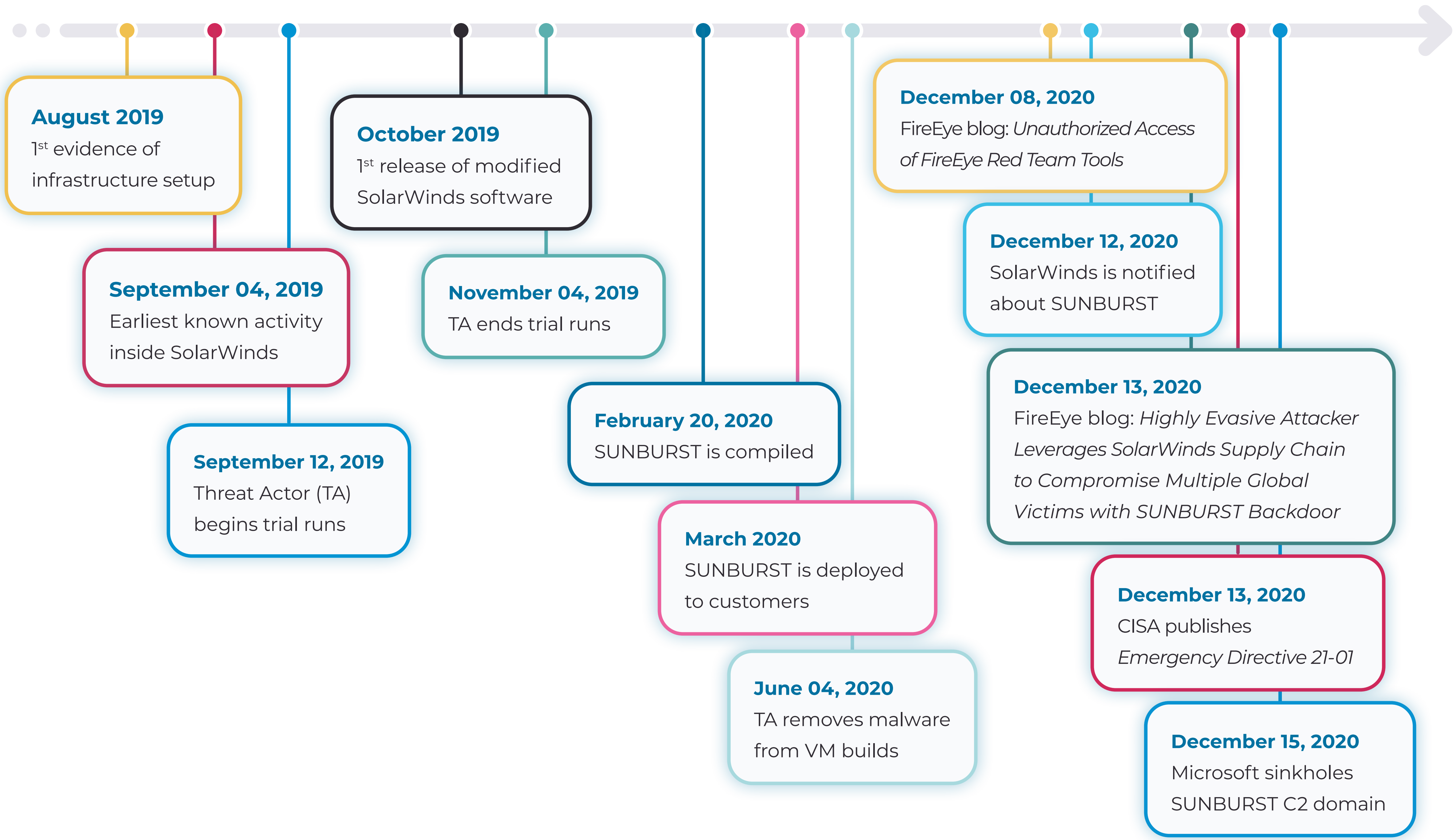
The list of affected customers includes government agencies, critical infrastructure and private sector organizations around the world. It is important to note that based on investigations so far, it seems that only a small fraction of customers receiving the backdoored update had additional second stage malware deployed in their infrastructure. This suggests that the goal of this calculated and methodical attack was to stealthily infiltrate the most interesting targets, while at the same time minimizing the likelihood of detection.

Given the ability to conduct a supply chain attack of this magnitude and the anti-forensics measures employed, the attacker demonstrated a remarkable level of sophistication and patience. These capabilities are typically associated with nation state actors.

Investigations regarding this campaign and its impact are still ongoing. Nonetheless, what we do know demonstrates the significant risks associated with supply chain attacks. They provide attackers with a single point of weakness to focus on, to gain access to a large number and variety of systems.

While disclosing the security compromise that led to the widescale deployment of SUNBURST, SolarWinds also revealed a second malware dubbed SUPERNOVA. At the time of this writing SUPERNOVA seems to be exclusively targeting SolarWinds' own network. No hard evidence linking the two malware programs has been published.

Solarwinds Timeline Diagram



August 2019
1st evidence of infrastructure setup

September 04, 2019
Earliest known activity inside SolarWinds

September 12, 2019
Threat Actor (TA) begins trial runs

October 2019
1st release of modified SolarWinds software

November 04, 2019
TA ends trial runs

February 20, 2020
SUNBURST is compiled

March 2020
SUNBURST is deployed to customers

June 04, 2020
TA removes malware from VM builds

December 08, 2020
FireEye blog: *Unauthorized Access of FireEye Red Team Tools*

December 12, 2020
SolarWinds is notified about SUNBURST

December 13, 2020
FireEye blog: *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*

December 13, 2020
CISA publishes *Emergency Directive 21-01*

December 15, 2020
Microsoft sinkholes SUNBURST C2 domain

3.1.3 MuddyWater

MuddyWater is an APT previously associated with espionage campaigns leveraging social engineering techniques. In September 2020, ClearSky Cyber Security reported several campaigns targeting organizations in Israel and other countries.[31] The campaigns leveraged TTPs associated with the Muddywater group and used two types of attack vectors for initial access:

- Social engineering
- Exploitation of the CVE-2020-0688 Microsoft Exchange vulnerability

Communication with external web services over SSL is used for C&C. Connecting with the C&C leads to a download of the PowGoop loader malware, which is subsequently used by the attackers to download additional files.[32]

Shown next are the techniques used by the threat actor described using the MITRE ATT&CK frameworks.

Phishing: Spearphishing Attachment
[T0865]

Obfuscated Files or Information
[T1027]

External Remote Services
[T1133]

Web Service
[T1102]

User Execution: Malicious File
[T1204.002]

3.1.4 MontysThree

A report about an APT group conducting focused industrial espionage against Russian-speaking targets was published at the beginning of October. While the attacks date back to 2018, some of the techniques and procedures used are unique to the recent use of the malware.

The targets were deduced to be companies in Russian-speaking countries based on hardcoded strings used in Cyrillic Windows locales. The malware uses legitimate public cloud services such as Dropbox and Google for its C&C, plus it heavily uses steganography.

Persistence is achieved by modifying existing .lnk files used for legitimate applications.

While the malware used by the group is not particularly advanced compared to state-sponsored APTs, it is an interesting example of a group focusing on industrial espionage.[33]

Web Service
[T1102]

Exfiltration Over Web Service
[T1567]

Masquerading: Match Legitimate Name or Location
[T1036.005]

3.1.5 Unnamed Campaigns Targeting Russian Industrial Enterprises

A report about a group conducting phishing campaigns against Russian industrial organizations was published in November. According to this report, most of the targets are in industries such as mining, logistics, energy, construction and oil & gas.[34]

The social engineering method employed was highly customized for each target. Email messages were crafted to appear as if they were coming from within the target organization or from a business associate.

Malicious attachments were occasionally disguised as legitimate documents containing industrial equipment configuration information, which are not something that the average attacker can access.

The payload installs an outdated version of TeamViewer, which is then modified to completely hide its interface from people using the machine by means of a malicious DLL. The attackers use a TeamViewer client to connect to the target and then start moving laterally within the network and exfiltrating data.

While the techniques used to gain an initial foothold and maintain access are rather simple, the level of social engineering displayed is quite advanced.

This particular threat actor seems to be primarily motivated by financial fraud.

Phishing: Spearphishing Attachment **[T0865]**

Hijack Execution Flow: DLL Search Order Hijacking **[T1574.001]**

3.1.6 Drovorub

A joint advisory by the FBI and the NSA was published in August describing and attributing the Drovorub Linux malware toolkit to Russia's GRU.[35] Moreover, Schneider Electric released a security bulletin on November 10, recommending a defense in depth approach to protect two of their products from the malware. The advisory details methods to detect Drovorub via memory analysis, host-based probing, and network traffic.[36]

Drovorub consists of:

- An implant
- A persistent kernel rootkit
- An agent providing file transfer
- Several port forwarding features
- A server component running on attacker-controlled infrastructure

JSON over WebSockets is used for communication between the different components. Detecting the presence of Drovorub can be challenging due to the anti-forensic techniques employed by the kernal rootkit to hide its presence in the file system, the network, and the process list.

Preventative mitigation steps include keeping Linux systems updated with the latest software versions and using a Linux kernel version that supports signed kernel modules. Untrusted kernel modules are often used by rootkits for execution.

Application Layer Protocol: Web Protocols **[T1071.001]**

Exfiltration Over C2 Channel **[T1041]**

Command and Scripting Interpreter: Unix Shell **[T1059.004]**

Rootkit **[T1014]**

3.1.7 Trickbot

The Trickbot botnet has been active since 2016 and is typically delivered through email campaigns. Trickbot has been the center of a lot of recent activity because of its somewhat unique characteristics.

By effectively operating a “malware-as-a-service” platform, its operators can sell access to infected machines. Customers could be common criminals looking for access to a monetizable target or even nation state actors searching for specific assets. This made Trickbot a very urgent concern during the weeks leading up to the U.S. presidential elections, and is the primary reason Microsoft acted in October. The company took legal action to shut down significant pieces of Trickbot infrastructure through a copyright claim. Furthermore, Microsoft and its partners pledged to continue targeting Trickbot should the operations restart.[37]

Given the level of sophistication displayed by the Trickbot operation, it is not surprising that there were measures in place to remain resilient in the face of possible takedowns.

The coordinated action led by Microsoft disrupted Trickbot C&C connections that relied on U.S.-based servers. However, the malware operators quickly set up new C&C infrastructure using infected MikroTik consumer routers in Europe, South America and Asia. The geographical distribution of the new nodes, in addition to the ease of provisioning them, makes the new C&C servers much more difficult to take down.

Phishing: Spearphishing Attachment **[T1566.001]**

Phishing: Spearphishing Link **[T1566.002]**

Fallback Channels **[T1008]**

Exfiltration Over C2 Channel **[T1041]**

NOZOMI NETWORKS BLOG

New Threat Intelligence Reveals Misuse of DNS Protocol

We have uncovered new misuse of the DNS (Domain Name Service) that is impacting corporate networks and opens the door to significant threats in the future.

The techniques involved include:

- Blockchain-based domain name resolution
- Misuse of the OpenNIC Alternative domain name service
- DNS over HTTPS (DoH)

It’s critical for security teams to leverage technologies that centrally inspect DNS traffic. If communications related to resolvers susceptible to misuse are detected (such as Emercoin or DoH), alerts should be raised, and defensive action taken.[38]

3.1.8 Bazar

Bazar is a modular malware platform that has two areas of functionality: a loader that is deployed as the result of a successful attack, such as a phishing email, and a backdoor that is used to establish persistence within a target.

Once the backdoor is successfully activated, it is typically leveraged to deploy additional payloads. Bazar has been seen dropping Cobalt Strike to ease lateral movement and, at a later stage, ransomware such as Ryuk once the desired level of access has been achieved.

Bazar is named after its use of .bazar domains, a naming scheme alternative to DNS based on the Emercoin blockchain. The use of a permission-less naming scheme is not completely unusual. Given the profile of Bazar's victims, however, this methodology is now subject to intense scrutiny by security teams.[39]

3.1.9 Ryuk

Ryuk is a notorious ransomware that has been active throughout 2020. During this time period it has been deployed at the end of successful Bazar compromises. What makes Ryuk particularly heinous is its targeting of healthcare facilities, which are already under extreme pressure while dealing with the COVID-19 pandemic.[40]

Ryuk also stands out for the speed of its attacks. Depending on the targeted network, the length of time from initial infection to ransomware execution can be as short as a couple of hours.

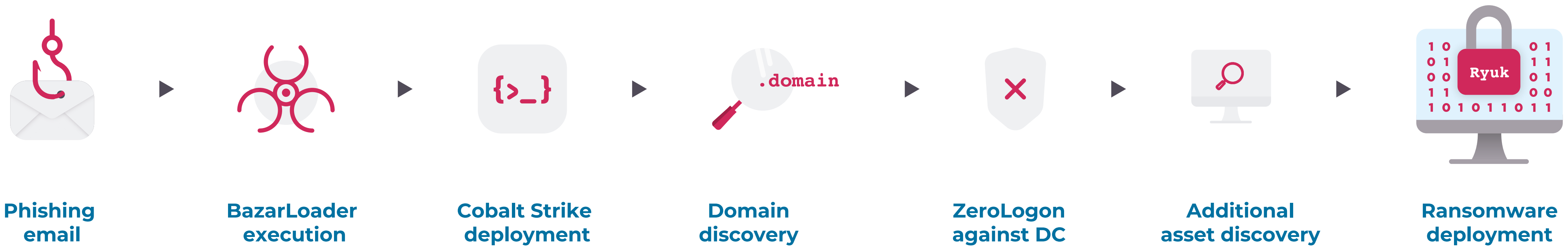
Data Encrypted for Impact
[T1486]

Loss of Productivity and Revenue
[T0828]

Ryuk is an example of a malware deployed by a determined gang that is relentlessly seeking out lucrative targets for large ransoms.

It is believed to be run by a professional crime group that has earned over $150 million USD in Bitcoin.[41]

Ryuk Kill Chain



Phishing email ▶ BazarLoader execution ▶ Cobalt Strike deployment ▶ Domain discovery ▶ ZeroLogon against DC ▶ Additional asset discovery ▶ Ransomware deployment

3.1.10 Cobalt Strike

Cobalt Strike is a paid software suite used to emulate threats and execute targeted attacks. It includes modules for reconnaissance, post-exploitation, covert communications, and real-time team collaboration. While predominantly used by companies for penetration testing engagements, Cobalt Strike's capabilities have attracted the attention of threat actors who use the toolkit when conducting attacks against corporate networks.

Specifically, many of the groups performing ransomware attacks leverage leaked Cobalt Strike versions to perform lateral movement and C&C communications. One example is the **Ryuk** ransomware group, who are behind a number of high-profile attacks against the healthcare, energy and government sectors.[42] While efforts have been taken by security researchers to detect the various components of the Cobalt Strike toolkit, it is an evolving modular framework. Consequently, the malware still evades identification by some detection methods.

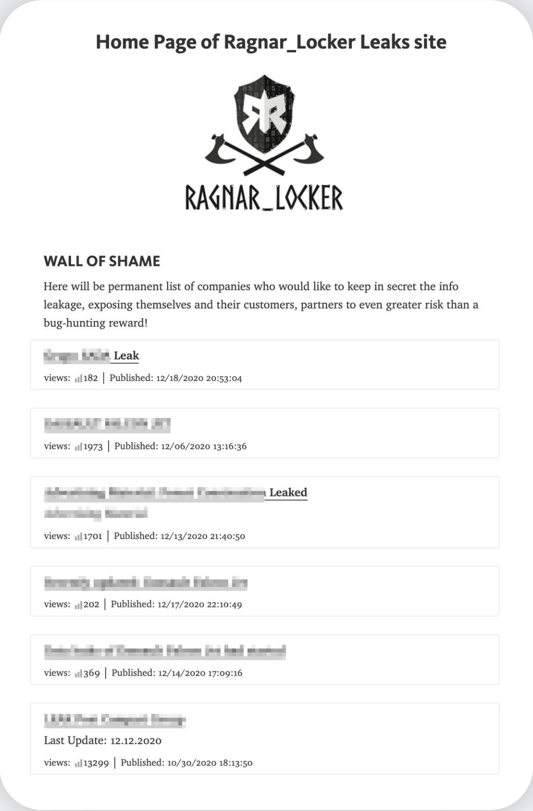
3.1.11 Ragnar Locker

Ragnar Locker is a ransomware that made headlines in 2019 after a series of prominent attacks against companies. One of the novel methods it uses to evade detection is to deploy a virtual machine that houses the utilities needed to perform encryption. This prevents host-based security software from monitoring it. Ragnar Locker operators, like most major groups nowadays, perform data theft prior to encryption. They use the stolen data as leverage to coerce the victim into paying the ransom, either by publicizing file samples or contacting the media.[43]

Data Encrypted for Impact
[T1486]

Loss of Productivity and Revenue
[T0828]

Hide Artifacts: Run Virtual Instance
[T1564.006]



Home Page of Ragnar_Locker Leaks site

WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

[redacted] Leak
views: 182 | Published: 12/18/2020 20:53:04

[redacted]
views: 1973 | Published: 12/06/2020 13:16:36

[redacted] Leaked
views: 1701 | Published: 12/13/2020 21:40:50

[redacted]
views: 202 | Published: 12/17/2020 22:10:49

[redacted]
views: 369 | Published: 12/14/2020 17:09:16

[redacted]
Last Update: 12.12.2020
views: 13299 | Published: 10/30/2020 18:13:50

The website of the Ragnar Locker criminal group lists victims of their ransomware attacks and provides links to their exfiltrated data.

Ragnar Locker Attacks

In November 2020 Ragnar Locker was responsible for an attack against an Italian company in the **branded beverage industry**.

Ransom was set to **$15 million USD in Bitcoin**.

The ransomware operators **threatened to release 2TB of data** they claimed was exfiltrated during the breach, providing samples as proof.

They also used a **hacked Facebook account** to run an advertising campaign, as an attempt to mock and coerce the company into paying the requested sum.

Furthermore, it became public that Ragnar Locker was implicated in another high-profile **attack against a Japanese game development company**.

3.1.12 Netwalker

The group behind the Netwalker ransomware continued to be busy during the second half of 2020. They attacked high-profile attack targets including Argentina's official immigration agency, universities, government institutions and companies in the cybersecurity, energy and health sectors.

The Netwalker group cashed out more than

$25M USD

in ransom between March and July 2020.[44]

A flash alert was released by the FBI in July to help security professionals and system administrators protect infrastructure against Netwalker.[45] The threat gang relies on emails (occasionally COVID-19-themed), weak RDP credentials, or exploits against VPN appliances to get initial access to a target network. After performing lateral movement, data is exfiltrated using popular cloud services like MEGA, and subsequently encrypted. The NetWalker group threatens its victims with data exposure just like most major ransomware operations.

Data Encrypted for Impact **[T1486]**

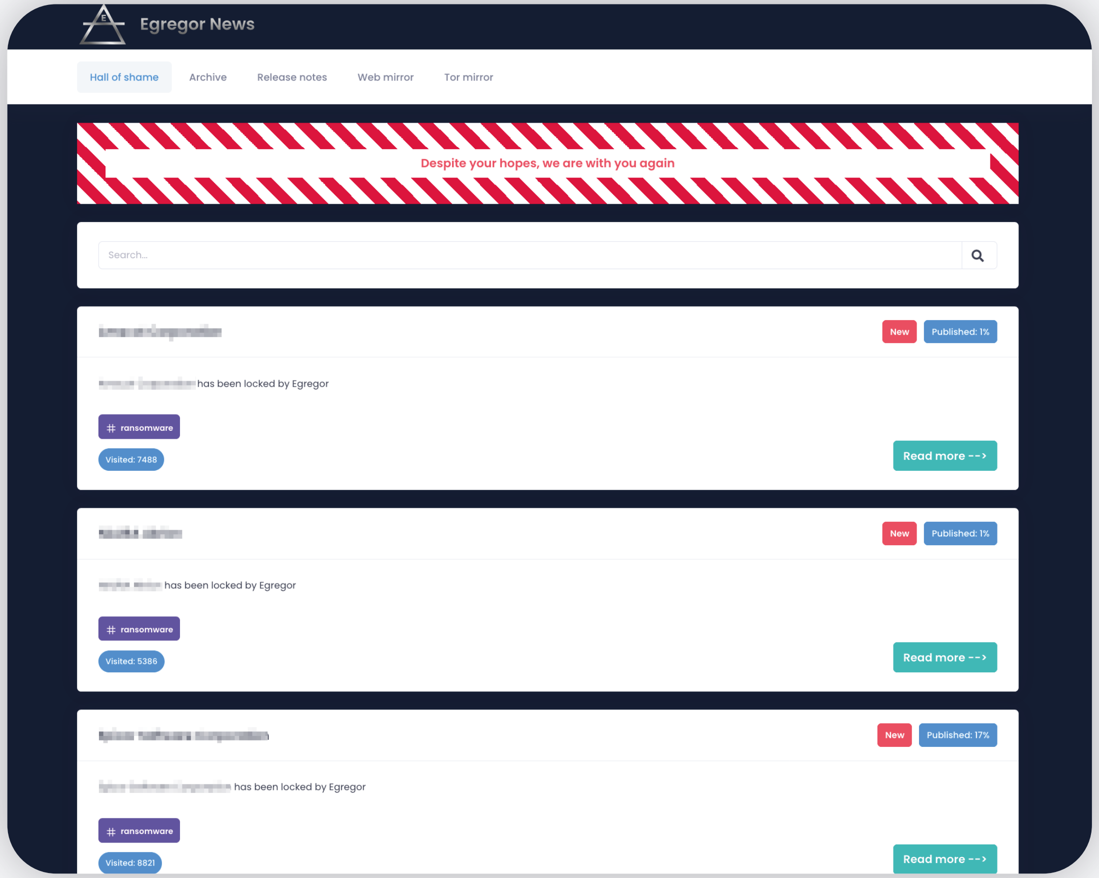
Loss of Productivity and Revenue **[T0828]**

3.1.13 Egregor

Egregor is a newly emerging ransomware that shows similarities to the Sekhmet ransomware. While it has only been active since September of 2020, it is already responsible for a successful attack against a South American retail giant. During the attack, data was exfiltrated and, curiously, printers were misused to print the ransom note.
The Egregor operators maintain a website running as a Tor hidden service, which displays information regarding their latest victims.

Data Encrypted for Impact **[T1486]**

Loss of Productivity and Revenue **[T0828]**



Despite your hopes, we are with you again

[redacted]

[redacted] has been locked by Egregor

[redacted]

[redacted] has been locked by Egregor

[redacted]

[redacted] has been locked by Egregor

The Egregor "wall of shame" proudly announces the organizations whose systems have been locked by its ransomware

3.1.14 Pay2Key

Based on an alert published by Check Point Research, many Israeli companies reported ransomware attacks by an unknown malware, later identified as Pay2Key.[46] The ransoms demanded were much lower than what the **Ryuk** or **Netwalker** groups typically demand. On the other hand, the Pay2Key operators showed skill in gaining an initial foothold and then rapidly spreading through target networks.

RDP seems to be the vector used for initial entry and PsExec was used to execute the ransomware on multiple machines within target organizations. Furthermore, the ransom notes were customized for each target. Like most ransomware groups, the Pay2Key group hosts a website running as a hidden service to publish exfiltrated data as an incentive for "cooperation." The bitcoin transaction trail left when some victims paid the ransom led to a cryptocurrency exchange based in Iran.[47]

Data Encrypted for Impact **[T1486]**

Loss of Productivity and Revenue **[T0828]**

External Remote Services **[T0822/T1133]**

3.1.15 Emotet

Active since 2014, Emotet is still a prevalent threat today. Specifically, CISA, in collaboration with MS-ISAC, published an alert notifying the public about increased Emotet-related activity.[48] While Emotet began its career as a banking trojan, it now functions primarily as a loader that puts additional malicious payloads on infected computers. To infect victims, Emotet leverages emails with malicious links or attachments, some of which used COVID-19-based themes.

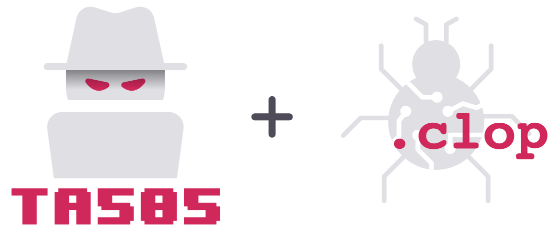
A technique recently introduced to Emotet is encrypting malicious attachments by archiving them with a password. When victims are tricked into extracting the attachments, the malware filters of email gateways are bypassed. Access to infected computers is rented out to other malicious parties who then proceed to install ransomware (like **Ryuk**) or tools to harvest financial information.

Phishing: Spearphishing Attachment **[T1566.001]**

Phishing: Spearphishing Link **[T1566.002]**

3.1.16 SDBbot

SDBbot is a remote access tool written in C++ typically used to move laterally within networks and exfiltrate data. It is associated with the TA505 threat actor and additionally the Clop ransomware.



On November 12, the Australian Cyber Security Centre (ACSC) published an alert warning about increased SDBbot activity targeting the Australian health sector.[49]

3.1.17 Mozi

Mozi (also known as Mozi.m) is a large botnet primarily comprised of routers and IoT devices. These so-called IoT botnets are typically used for tunneling, or to launch DDoS attacks. Mozi's nodes are constantly scanning the internet for devices that use weak telnet credentials or that are susceptible to several vulnerabilities the botnet can exploit.

Mozi uses a P2P architecture based on a DHT-based protocol and relies on existing DHT infrastructure typically used for BitTorrent. This approach is interesting, as it makes it easier to set up the initial P2P network and prevents the casual observer from noticing its traffic.

The C&C architecture and the geographical distribution of its nodes makes takedown attempts difficult. The malware, once deployed on vulnerable devices, supports several DoS attacks – a classic IoT botnet strategy.

Exploit Public-Facing Application
[T1190]

Valid Accounts: Default Accounts
[T1078.001]

Brute Force: Credential Stuffing
[T1110.004]

Application Layer Protocol
[T1071]

Traffic Signaling
[T1205]

NOZOMI NETWORKS BLOG

Overcoming the Challenges of Detecting P2P Botnets on Your Network

Threat actors use peer-to-peer (P2P) botnets to build a platform for carrying out malicious operations. Understanding the architectural designs and emerging techniques of recent botnets helps us use network artifacts to detect and mitigate their activity.

We explored:

- The recent evolution of botnet platforms
- Why peer-to-peer botnets are challenging to disrupt
- DDG botnet
- FritzFrog botnet
- Mozi botnet

The important takeaway from our analysis is that botnet operations give security defenders multiple starting points for investigating the network artifacts they leave behind. This information can then be used to inform mitigation efforts.[50]

3.1.18 Moobot

Moobot is a self-propagating botnet that targets exposed IoT devices and uses them for malicious activities like DDoS. The botnet propagates by leveraging weak telnet credentials and exploits online consumer devices such as routers, NVR, DVR and IP cameras.

Moobot's codebase shows similarities to Mirai, a notorious IoT botnet whose source code became public back in 2017 and gave rise to many variants. It is worthwhile to note that Moobot was seen using two exploits before either of them were public – the Netlink GPON Router 1.0.11 RCE exploit and an additional exploit targeting various CCTV NVR/DVR devices.[51] This indicates that the botnet's developers either have the resources to gain access to zero-day exploits from the market, or the technical expertise to perform independent vulnerability research. These capabilities set them apart from the average IoT botnet operator.

In September, Cloudflare published a report about a UDP-based DDoS attack peaking at 654 Gbps and lasting 2 minutes.[52] It is believed to have been initiated by the Moobot botnet. The attack originated from 18,705 unique IP addresses located in 100 countries, which is rather large for this type of botnet.

UDP-based DDoS Attack

Peak
654 Gbps

Duration
2 Minutes

Unique IP Addresses
18,705

IP Addresses Located in
100 Countries

The vast majority of the IPs were based in the U.S., South Korea, Japan and India. While that particular attack was successfully mitigated, it is important to note that DDoS attacks of this scale can easily disrupt services or access to infrastructure. This is especially problematic now, taking into consideration the high number of businesses, organisations and educational institutions operating remotely.

Exploit Public-Facing Application
[T1190]

Valid Accounts: Default Accounts
[T1078.001]

Brute Force: Credential Stuffing
[T1110.004]

Network Denial of Service
[T1498]

4

Vulnerability Overview

4.1 Introduction

Assessing the relative impact of new vulnerabilities released in a given timeframe is a constant challenge for every security team. A practical approach is to consider the attack surface exposed by essential services and evaluate the consequences of it being compromised through exploitation of new vulnerabilities.

Analyzing the new vulnerabilities released by ICS-CERT helps organizations understand which ICS devices or software, and their weaknesses, have recently come under public scrutiny. Still, this exercise will result in only a partial grasp of the actual risks faced by a company.

To provide better context and more actionable information, we include two special sections. In the first, we describe recently emerging trends that we believe will apply for the foreseeable future. In the second, we highlight vulnerabilities observed in the wild during the timeframe of this report, regardless of when the actual discovery took place.

In a threat landscape where ransomware organizations are attacking companies indiscriminately, it's vital to understand your exposure to vulnerabilities under active exploitation. At the same time, nation state threat groups have been observed using non-zero-day exploits in their operations. In this realm, the NSA is showing leadership by releasing specific advisories detailing how Chinese and Russian state actors are using known vulnerabilities to compromise multiple networks.

4.1.1 Analysis of ICS-CERT Advisories

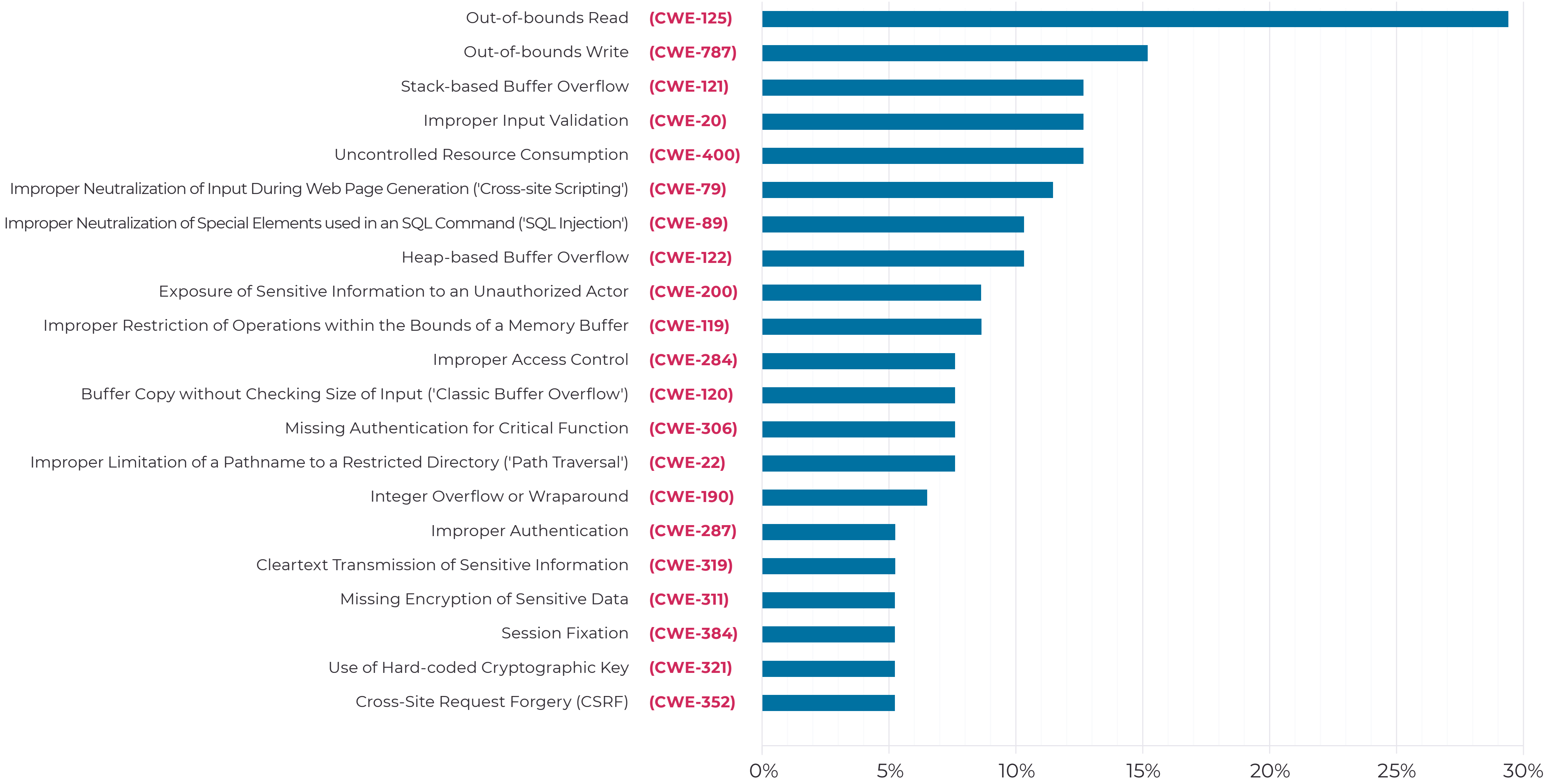
ICS-CERT, a program run by CISA, a U.S. government body, publishes advisories on ICS vulnerabilities, exploits and security issues. It utilizes the Common Weakness Enumeration (CWE) classification system for software and hardware vulnerabilities developed by MITRE.[53]

In the second half of 2020, we analyzed a total of 151 ICS industrial advisories and 13 ICS medical advisories containing new vulnerabilities. We further classified the CVEs according to the assigned CWE categories. CWE is very useful in providing a taxonomy for vulnerabilities but is just the starting point for properly assessing the impact of a security issue.

Memory corruption errors such as CWE-125, CWE-787, and CWE-121 continue to represent a large portion of the new vulnerabilities described in industrial advisories. This will likely continue, considering that the software stacks of many assets in ICS environments were not designed with today's connectivity in mind and its consequence in terms of security exposure.

ICS medical advisories, by contrast, have a predominance of improper authentication CWE-287 vulnerabilities. The number of ICS medical vulnerabilities is too low, however, to assume this is a meaningful trend. Analysis is further limited by the constrained access that security researchers have to medical devices. These gaps do not mean, however, that medical devices are inherently safer than other ICS devices.

Common Industrial Device Vulnerability Types



Nozomi Networks evaluated 151 ICS-CERT advisories and the >270 specific vulnerabilities they described. We classified this detailed information into CWE categories and show the most prevalent vulnerability types in the chart above.

ERROR

Memory corruption errors continue to represent the largest percentage of new vulnerabilities described in ICS advisories.

Together, CWE-125, CWE-787, and CWE-121 accounted for 58% of vulnerability types.

We expect this situation to continue as the software stacks of many ICS assets lack intrinsic security and receive limited security oversight.

4.2 Vulnerability Research and Exploitation Trends

4.2.1 Software Supply Chain

Though not a new concept, software supply chain vulnerability research and exploitation is the most important trend of recent months.

Threat actors study supply chains to find vulnerabilities, and then exploit an embedded component commonly used in software stacks, or compromise a widely used software or service.

If the targeted component or software is relatively obscure, it might not have received the same level of security scrutiny as well-known software, increasing the attacker's chance of success. The more critical the functionality of the component or service, the more serious the security issue.

In the latter half of 2020, two types of supply chain scenarios were predominant. The **Ripple20** vulnerabilities are an example of an embedded component supply chain risk. JSOF identified 19 vulnerabilities in the TCP/IP stack from Treck, used by a wide variety of assets, and demonstrated a remote code execution exploit against a UPS. Later, however, it was shown that there is little chance that many targets meet the requirements needed for exploitation by a motivated threat actor.

The operation that compromised software developed by **SolarWinds** also falls under the software supply chain umbrella. In this case, compromise of a widely used software led to a successful attack against thousands of private and public U.S. organizations. This attack highlights the risks to end users who have limited agency over the software or services used within their networks, yet are directly impacted by their compromise.

NOZOMI NETWORKS BLOG

CISA Alert: Sophisticated, Ongoing Cyberattacks Go Beyond SolarWinds

Reports of Advanced Persistent Threat (APT) cyberattacks have indicated a scale and complexity that sets a new bar for potential threat impact. CISA has issued an alert warning that the initially identified access vector, a compromise of SolarWinds Orion platform, was not the only one.

The new CISA alert helps us understand:

- The scope and severity of the APT cyberattacks
- The colossal challenge of compromise identification and remediation
- The extreme complexities and consequences of the APTs

Nozomi Networks customers can determine if they are compromised using their network traffic for the period of March through June 2020. Assessing this traffic with our Threat Intelligence service, which detects all known IoCs (such as malicious traffic signatures, IPs, and domains) related to the attacks, will identify a breach.[54]

Supply chain attacks, therefore, are a very broad topic, and their actual impact on the security posture of a network depends on a case-by-case evaluation. Furthermore, defending against this kind of threat is a difficult task with no immediate solution.

A plausible first step would be to document the attack surface exposed by third-party providers of components embedded in critical software stacks, and services or software with privileged access to networks. Given the complexity of modern environments, this is by no means a small feat—it would require a major investment for any organization.

4.2.2 Licensing Software

Licensing software is an important component in many OT networks, used to enforce the licensing policies of many systems involved in automation processes. It is typically deployed in the form of a network service that connects with remote software for license management. These intrinsic characteristics make licensing software a sought-after target for attacks on OT networks.[55]

The names of licensing software processes have been found in ransomware kill lists, most notably Ekans, highlighting the critical nature of these systems.[56] Since a licensing server can reach valuable systems in the network, it represents a privileged launchpad for further attacks. Depending on how a system is configured, if the license server becomes unreachable, automation functionality might degrade or be halted altogether.

2020 is not the first time that licensing software has been the target of security researchers. Most notably, in 2018, a vulnerability was found for the AVEVA Wonderware License Server and reported to ICS-CERT.

During the timeframe of this report, Wibu-Systems' CodeMeter, a third-party license management system used by Rockwell Automation, Siemens and others, was the subject of an extensive assessment. Several high-risk vulnerabilities were identified, creating a particularly dangerous situation. CodeMeter is a component in the software of many automation vendors, and ICS software is often left unpatched for long timeframes, significantly increasing the window of exposure. High-profile vulnerabilities were also found in the ABB Central Licensing System, although in this case, without the same supply chain consequences.[57]

5 Notable Vulnerabilities

5.1 Synopsis of 7 Types of Vulnerabilities

5.1.1 Vulnerabilities Exploited by Chinese State-Sponsored Threat Actors

In October, the NSA released an interesting advisory outlining a list of publicly known vulnerabilities being exploited by Chinese state-sponsored threat actors. The targets were the networks of the U.S. National Security Systems, the Defense Industrial Base, and the Department of Defense.[58]

The vulnerabilities in question pertain to:

- Externally accessible protocols such as RDP, DNS, SMTP
- Networking equipment commonly found in corporate networks, such as routers, VPNs, and load balancing products

The importance of this list is twofold. First, it provides a breakdown of the most sought-after targets, which should be properly secured and monitored. Second, it emphasizes the importance of properly managing key IT assets by applying important security patches in a timely manner.

The general structure of the attacks followed a common pattern. The threat actor gained their initial foothold by exploiting one of the external remote services or via spearphishing attachments. Then they relied on vulnerabilities like CVE-2020-1472 to compromise Active Directory services and perform lateral movement. Persistence was achieved by abusing valid credentials to leverage legitimate external services.[59]

External Remote Services
[T1133][T0822]

Exploit Public-Facing Application
[T1190]

Spearphishing Attachment
[T1566.001][T0865]

5.1.2 Vulnerabilities Exploited by Russian State-Sponsored Actors

In December, the NSA released a further advisory detailing how Russian state-sponsored actors have been exploiting a vulnerability tracked as CVE-2020-4006. It affects a series of VMware products.

To exploit the vulnerability, the attackers required network access to an administrative webpage of the target, along with a valid password.

According to VMware, it was the NSA itself that disclosed the vulnerability to them.[60]

October 2020

NSA released a list of publicly known vulnerabilities being exploited by **Chinese state-sponsored threat actors**.

December 2020

NSA released a further advisory detailing how **Russian state-sponsored actors** have been exploiting a vulnerability tracked as CVE-2020-4006.

5.1.3 ZeroLogon (CVE-2020-1472)

CVE-2020-1472 is a critical vulnerability in the Netlogon Remote Protocol. Unauthenticated attackers can use it to obtain domain administrator privileges on a target domain controller (DC). Microsoft published the required security updates to manage the vulnerability in two phases. The initial phase was deployed on August 11, 2020, with a with a subsequent update released on February 9, 2021. This vulnerability is particularly concerning due to the ease with which it can be exploited by unauthenticated attackers to completely compromise local Windows networks.

According to an alert published on October 9 by CISA, APTs have been observed leveraging this vulnerability. The APTs have performed lateral movement by obtaining access to Active Directory servers.

Unfortunately, with vulnerabilities like this one, remediation is not as trivial as installing an update. Instead, it is important to follow the vendor's recommended steps (such as updating, monitoring event logs etc.) to correctly manage the possible risks.[61]

CISA ALERT, October 9, 2020

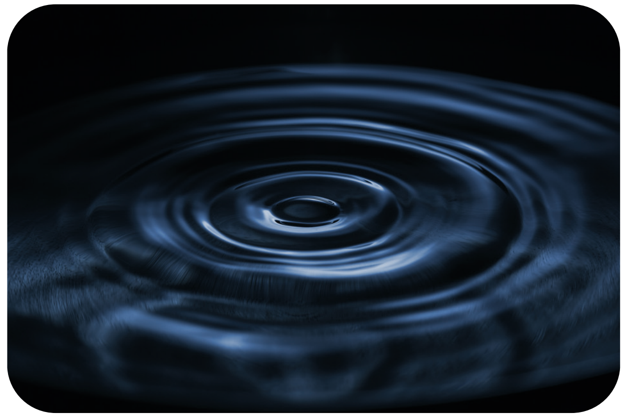
APTs have exploited ZeroLogon and performed lateral movement by obtaining access to Active Directory servers.

Just a few weeks after being disclosed,

ZeroLogon was exploited by APTs and ransomware organizations.

5.1.4 Ripple20

Ripple20 is a collection of 19 vulnerabilities disclosed by the security company JSOF in June. It affects the TCP/IP stack developed by Treck. The importance of this set of vulnerabilities lies in a series of facts that highlight the fragility of software supply chains.[62]



First, this TCP/IP stack is found in a wide variety of devices from printers to UPSes (uninterrupted power sources). In some cases, the manufacturer of the device has bought the full operating system from another vendor and are not aware of its software components. Furthermore, since the Treck business model involves the sale of the source code, some vendors customized the TCP/IP stack, effectively forking it. The impact was that some vendors did not integrate security patches into the TCP/IP code.

In addition, since the original set of vulnerabilities affected different versions of the Treck stack, understanding the actual exposure of a specific device proved to be extremely challenging. Although JSOF demonstrated a remote code execution exploit against a UPS, it was not clear at the time if widespread exploitation of these vulnerabilities was achievable in real world scenarios.

In October, supply chain security company Finite State released research on the actual risks posed by the Ripple20 vulnerabilities, based on a set of devices of their choosing.[63]

The outcome is that due to the variety of Teck stack configurations found on real devices, the likelihood of a widespread damaging attack is low. Several devices are not affected by some of the most serious vulnerabilities and each target requires specific customizations. The takeaway from this finding is that the prioritization of security patching needs to take into consideration the specific context of each risk.

5.1.5 AMNESIA:33

AMNESIA:33 is a series of vulnerabilities affecting a number of open-source embedded TCP/IP stacks. Assessing the impact and exploitability of the vulnerabilities is challenging due to the different features and configurations of the stacks that each vendor enables in their products.

This is another example of how vulnerabilities in third-party code can potentially affect a diverse set of devices through the supply chain. Having a deep understanding of the exact software components that a specific device or piece of software relies on can prove to be challenging, even for manufacturers. This series of vulnerabilities further highlights the risks that opaque supply chains pose.[64]

5.1.6 Solaris SSH RCE (CVE-2020-14871)

On November 4, FireEye's threat research team published a blog post describing a series of incidents affecting Oracle Solaris servers. Based on the artifacts, the initial compromise was performed by exploiting CVE-2020-14871, a stack-based buffer overflow vulnerability in the PAM library, which was remotely reachable via SSH by unauthenticated attackers.[65]

The vulnerability impacts Solaris 9, Solaris 10, Solaris 11 and certain versions of the Illumos OS. It is not often that we see easily exploitable remote code execution vulnerabilities for UNIX-based operating systems like this one.

While Oracle has released patches for Solaris 10 and 11, no patches were released for Solaris 9, which is unsupported. This situation once again underlines the importance of keeping up with vendor advisories and using possible workarounds if patches cannot be immediately deployed. Moreover, it is a reminder that there are threat actors with the capability of gaining access to zero-days, which may be used in the wild to attack target networks.

It is interesting to note the level of sophistication displayed by UNC1945, the group exploiting the aforementioned vulnerability in the wild. Not only did it have access to a Solaris zero-day, but it also employed several anti-forensics techniques to evade and thwart analysis. This threat group also displayed high technical aptitude by stealthily navigating the various operating systems in targeted networks.

External Remote Services
[T1133]

Exploit Public-Facing Application
[T1190]

SSH
[T1021.004]

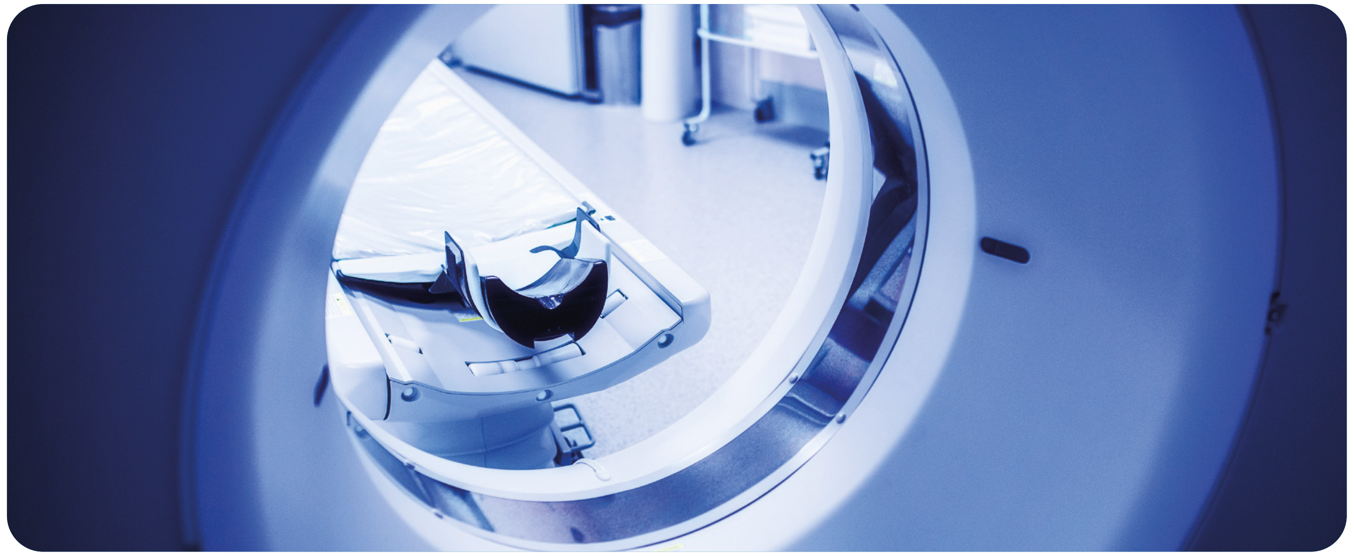
Threat group UNC1945's use of the Solaris SSH remote exploit demonstrates that **advanced attackers have a wide array of capabilities, well beyond traditional skills.**

5.1.7 GE Healthcare Imaging and Ultrasound Products Default Credentials

In December, security company CyberMDX released an advisory related to a set of credentials used extensively in many GE Healthcare imaging and ultrasound products.[66] The vulnerability lies in the fact that this set of credentials is used by GE Healthcare maintenance software to access devices through the internet, using insecure protocols.

The situation is complicated further by the fact that such credentials can only be changed by GE Healthcare through a request initiated by the customer. In addition, the credentials can be found online, along with some background information on the subject. The vendor reports that no incidents have been documented in clinical settings.

Valid Accounts: Default Accounts **[T1078.001]**



The security posture of medical devices is often weak across the healthcare industry.

Reducing the attack surface of medical devices should be the highest security priority for healthcare organizations.

6

Recommendations

6.1 Actionable Insights

Improving the security posture of an organization in the face of ever-emerging new threats cannot be summarized in a one-size-fits-all list of advice or principles. Every company has a unique set of requirements depending on the way it evolved over time, or the regulations for its industry.

The goal of this section is to provide a summary of recommendations that covers general-purpose suggestions that could be applied by many organizations, as well as more niche techniques. The latter address recent threats that might require a more mature security program for their implementation.

6.1.1 Network Monitoring

Network monitoring is a foundational element of mature security programs for IT networks but is in the adoption phase for OT and IoT environments. Network monitoring tools for industrial and critical infrastructure operations are specially designed to monitor the unique assets, communications and processes of control systems.

Thinking about the changing threat landscape, network monitoring helps defenders by identifying early-stage infection and reconnaissance activities. Behavior-based anomaly detection, which detects activities outside the normal pattern for a system and its control process, identifies changes such as irregular commands and new connections.

This should prompt security engineers to investigate further, using the rich analysis toolset available in the best OT/IoT monitoring solutions. This might include building sophisticated security primitives to tailor network oversight for the specific security processes of an organization. For example, being able to write rules that detect specific data and events from a stream of network traffic. These can be used as a threat hunting tool and updated over time to check various data flows for signs of infection and irregular behavior.

Further down the kill chain, monitoring tools help identify malware preparing for further propagation. During this phase, anomaly detection identifies new commands in the host network and generates alerts that include command sources. Even if the malware uses regular industrial protocols to communicate, its messages will vary from the system's baseline behavior, allowing them to be singled out.

If an attack occurs, it is quickly identified and alerts are sent out. This enables defenders to contain the attack through actions such as new firewall rules, or further actions to stop the malicious behaviour.

Good cybersecurity is a process where humans and tools interact to provide the strongest possible defense. Utilizing network monitoring is a practical way to automate and accelerate threat detection, improving defenses against emerging threats.

6.1.2 Attack Surface Reduction

Carefully understanding the scope of the attack surface available to threat actors is one of the first steps that any security team should perform. Attack surface reduction, in the context of OT/IoT infrastructure, is the set of measures required to limit the exposure of services to only those strictly required for the business to function properly.

This concept applies to systems accessible from the open internet, to limit the probability of a remote attacker gaining a foothold within a network. It also applies to systems internal to a network, to reduce the opportunity for lateral movement of threat actors.

Once this methodology has been applied at the infrastructure level, it can be further employed at the granularity of single applications. For example, limiting the functionality available in authentication and authorization programs.

In July, the NSA and CISA released an alert to asset owners and operators of critical infrastructure to help them reduce exposure of their OT systems.[67] This highlighted the trend of critical infrastructure increasingly becoming the target of malicious activities. The alert is particularly informative, providing a list of actionable items that any organization should carefully evaluate.

6.1.3 Network Segmentation

Network segmentation is probably the most basic, but often overlooked, tool in the arsenal of any security team. The way a network is segmented sometimes reflects the way an organization has evolved and established itself over the years. A network that was initially thoughtfully designed can have issues handling needs that arise later. For example, agile production changes, the shift from an office-based workforce to a remote-first situation, or acquisitions and the following integration phase.

On occasion, moving some services from an on-premises solution to a cloud-based one could indirectly help by taking some of the complexity out of the picture entirely. Unfortunately, this option might not be available for many OT networks given the peculiarities of the assets involved. Thus, with resilience requirements in mind, a proper segmentation should always be considered the cornerstone of a secure OT/IoT network.

A further example of the importance of this concept is evident if we look at the network from the perspective of an attacker. An external actor that wants to reach an internal asset will abstract the network implementation in the form of a graph. Any additional hop required to achieve the goal should cost a significant amount of effort, and simultaneously increase the chance of being detected.

6.1.4 Identity and Access Management (IAM)

IAM is another central piece of the puzzle of a secure organization. Most companies with a robust security program in place have an IAM solution already deployed. The transition towards more services being hosted in the cloud could represent a challenging situation, however, and one with security implications. A hybrid IAM solution with both an on-premises and cloud component might not always map nicely to the heterogeneity of some OT environments, leading to inadequate trade-offs.

The convergence of OT and IT is in fact bringing to the surface a well-known situation for many organizations, namely the presence of fragmented IAM implementations often managed by different departments. The consequences of this reality are twofold. On the one hand the lack of comprehensive traceability increases the overall risk posture. On the other hand, there could be compliance standards or more general legal requirements that force organizations to implement a unified IAM system.

The most comprehensive public analysis of IAM in the context of OT is still NIST Cybersecurity Practice Guide, Special Publication 1800-2: "Identity and Access Management for Electric Utilities," released in July 2018.[68] The focus on a practical approach, together with concrete examples of deployments for real world scenarios, makes this publication particularly useful.

6.1.5 Disaster Recovery Planning

Based on the lessons learned from ransomware attacks during the past few years, there are several disaster recovery planning steps that should be carefully considered.

A characteristic case study would be Norsk Hydro, one of the largest aluminum companies. Norsk Hydro was affected by a ransomware attack in 2019, which forced the company to halt around 170 plants. An employee clicking on a malicious email set in motion a chain of events that impacted 35,000 employees across 40 countries. The company refused to pay the ransom and relied on external platforms like Facebook and WhatsApp for communication.

Additionally, Norsk Hydro chose to be completely open and transparent about the situation by providing frequent updates to the public.[69] Specifically, they held daily press conferences, delivered webinars, and launched a new website to interact with the external world. This approach was widely praised by the security community.

Companies should focus on preventing successful breaches in the first place by following security best practices and educating their employees on security hygiene. That being said, a proper disaster recovery plan should be in place to handle scenarios where multiple computer-based systems are affected simultaneously and production is dropped or halted completely. Ransomware groups often remain inside target networks for extended periods of time, moving laterally to maximize their impact. Global organizations should thoroughly consider how they would handle disruptions impacting multiple geographies at the same time.

6.1.6 Active Directory Hardening

Based on the threats and attacks examined earlier, it is clear that attackers often rely on Active Directory to enable lateral movement inside a compromised network. In the case of ransomware attacks, the goal is to maximize impact by deploying the malware to as many workstations and servers as possible.

To secure your Active Directory system:

- Use current Windows versions for Domain Controllers and restrict software applications to as few as possible to reduce the attack surface
- Use AppLocker to limit the applications allowed to run in a Domain Controller
- Secure built-in administrator accounts by reducing them and minimizing their privileges
- Tighten the default Domain Policy GPO password policy (length, complexity, lockout thresholds)
- Monitor Windows event logs for suspicious events (4618, 4649, 4719, 4719, 4766, 4794, 4897, 4964, 5124 etc.) that could indicate compromise
- Disable WDigest authentication in earlier Windows versions[70]

6.1.7 Secure Remote Access

The drastic shift from offices to remote work poses several difficulties for security teams. They are tasked with balancing employee productivity while managing the risks that remote access to internal infrastructure brings to the table. Based on a report published by Gartner in July, 48% of employees will continue to partly work from home post-COVID-19, and around 20% will work remotely full-time.[71]

While companies must continue to handle the new work patterns, opportunistic threat activity against the vulnerable public is on the rise. According to a report published by researchers from the University of Cambridge, who analyzed the activity of a cybercrime market for a period of 14 months, overall market volume rapidly increased during the pandemic.[72] The results of this study can be partially attributed to the market's participants having an increased amount of free time (due to school closures or lay-offs) to engage in cybercrime. Nonetheless, the overall changes in infrastructure, along with the general climate of unease and unrest makes organizations ripe targets for exploitation.

While companies forced to move forward with a remote workforce were at different levels of preparedness when the pandemic began, there are various steps that all can take to improve cyber resilience going forward.[73]

First and foremost, only devices that are uniquely identifiable and actively managed should be used to access internal infrastructure. Authentication for VPNs and appliances should force users to pick strong passwords and make use of multi-factor authentication. Once a user is connected to the network, access controls and strongly enforced policies should be used to minimize accessible endpoints. Moreover, access to any external services should be logged and monitored carefully to detect any breach attempts or anomalies.

While remote access appliances are usually essential, they can also be a fruitful source of vulnerabilities for threat actors to exploit. For example, vulnerabilities like CVE-2019-11510 and CVE-2019-19781 have been extensively abused by various actors, so threat models should carefully evaluate this type of risk.

For some companies, it might be valuable to follow approaches like the Zero Trust holistic model to security, where the focus is on users, assets and resources rather than a static network-based perimeter. While it can be challenging to deploy and migrate to such an architecture without impacting business continuity or user productivity, useful case studies by enterprises like Microsoft and Google, detailing their experiences, are available.[74]

6.1.8 Detection of Blockchain-based Infrastructure

The usage of blockchain-based infrastructure by malware is certainly not a new concept. Since the introduction of the first naming schemes based on a blockchain, such as Namecoin, malware operators started experimenting with permissionless naming schemes. These schemes provide a powerful alternative to DNS, a system managed by a central authority called a registrar. In a blockchain-based naming system, registering a new domain or updating an existing one involves issuing a transaction within the blockchain of reference, without any third-party interference.[75]

The downside of this technique is that regular DNS servers do not resolve domain names bound to blockchains. To perform a name-to-IP resolution, malware relies on either well-known and established DNS services such as OpenNIC, or on ambiguous DNS servers that are capable of performing the required mapping.[76]

Though they provide convenient features and reduce complexity, **remote access appliances provide an extremely attractive attack surface for exploitation by threat actors.**

In the context of a corporate network, these alternative DNS servers (even if legitimate as in the case of OpenNIC) should not be allowed. Security teams should actively block both the resolution of domain names belonging to blockchain-based naming systems as well as the IP addresses of known DNS servers that resolves these names.

6.1.9 DNS over HTTPS

DNS over HTTPS, or DoH, is a protocol that, as name suggests, allows the resolution of domain names over HTTPS. While DoH is not a novelty per se, there is evidence that more malware is using the protocol. The uses include both resolving the names of the hosts involved in malicious infrastructure, and as a cover channel to exchange information through public resolvers.

Security researchers started experimenting with DoH as early as 2018, and in 2019 we had the first occurrence of malware actively abusing the protocol. In August 2020, security company Huntress identified a new malware leveraging the Google public DoH resolver to fetch the IP addresses of further pieces of infrastructure through DNS TXT records.[77]

DoH is supported in different shapes and forms by Firefox, Google, Microsoft and Apple. The deployment of this technology is evolving rapidly and security teams need to evaluate how this type of risk impacts the cyber resilience of their environment. In particular, consider the scenario where DoH breaks and allows threat actors to transparently inspect the DNS traffic traversing your networks.[78]

6.1.10 Awareness of Legitimate Online Service Abuse

The abuse of legitimate online services has always been a difficult vector to defend against and a textbook example of why defense in depth is so important. Services such as storage, URL shorteners, or online word processors often play a decisive role in the chain of events that leads to a compromise. They typically exploit the trust that end users have for recognized brands. We can broadly distinguish amongst this group of threats based on the goals of the malicious actor.

Most of the attackers leverage online services in a process that delivers a malicious payload to the target. This is done by using a trusted service to host either the final deliverable or a link that leads to the payload. The operators of Bazar loader/backdoor took this approach even further in July 2020.[79] They used the email marketing platform Sendgrid to launch a spam campaign which contained a link to a maliciously infected document hosted on Google Docs. The use of Sendgrid allowed the attackers to reach a larger number of end users than a less trusted email server would.

A second, more niche abuse of legitimate services takes place during the reconnaissance phase that precedes an attack. A malicious operator can use a marketing service that exposes the operating system and browser version used by a target, and thus customize its toolset accordingly.

During the buildup to the 2020 U.S. presidential election, a nation state actor tracked by Microsoft used a similar approach to verify the usage of targeted email addresses. By registering a new domain and sending links to it through focused emails, the actor gathered useful information for the next steps of the attack. This type of abuse is the most complicated to counteract, and is often discovered only in the post-mortem of an incident.

In the last few years, online services have been compromised in ways their creators and adopters never dreamed of. Fortunately, we've also seen several of the companies behind these services reacting and deploying successful strategies against this situation.

Security teams should assess the services allowed within an organization for their potential for abuse. This includes evaluating the security posture of the vendor and whether or not there's a point of contact that can be reached if an incident occurs.

7

Conclusion

7.1 Supply Chain and Persistent Ransomware Attacks Reach New Heights

This report highlights the threats and vulnerabilities that were important since July 2020. Understanding these risks provides insight into the evolving threat landscape and how it can best be approached by security teams. As supply chain and persistent ransomware attacks increase, it is crucial to continuously improve cyber resiliency. To do so requires full visibility of all IT, OT and IoT assets and up-to-date threat and vulnerability information.

The SolarWinds breach is a dramatic and instructive example of the significant risks of software supply chain attacks. Whether an attack succeeds in compromising an embedded component, a widely used service or software, or a supplier's network, the impact on companies further down the supply chain can be momentous. Defending against this kind of threat is a difficult task and speaks to the need for attack surface reduction, good network segmentation and high cyber resiliency.

Ransomware attacks will persist as a dominant risk and your organization should ensure that security teams have up-to-date OT and IoT threat intelligence for ongoing threat modeling and risk assessment. They should also be prepared to act quickly if a breach occurs, and work hand-in-hand with other business groups, such as finance, legal, compliance and communications for disaster recovery.

Memory corruption errors will continue to be the dominant type of vulnerability for industrial devices. Monitoring ICS-CERT advisories, prioritizing vulnerability risks and patching or mitigating to combat the top risks are a cornerstone of any industrial security program.

The pandemic economy is speeding up the adoption of cyber-physical systems, making it more important than ever to secure operational technology systems. 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.

Gartner

> **"As cyber-physical systems continue to multiply due to IT/OT convergence or IoT/industrial IoT (IIoT)-type deployments, they increase and blend risks in the cyber and physical worlds... Bad actors increasingly target weaknesses wherever they are, as demonstrated by the surge in ransomware affecting organizations' operational systems."**

The right technology and threat information can greatly assist by providing integrated information that eliminates blind spots. For example, the Nozomi Networks solution significantly advances OT/IoT visibility and cybersecurity, plus it integrates with IT tools and processes.

Our solution automatically creates a current inventory and visualization of all assets in OT and IoT environments, revealing the complete attack surface. It delivers ongoing threat and vulnerability intelligence that reduces both the mean-time-to-detection and the mean-time-to-response. It also monitors behavior for anomalies and threats, and alerts security teams to changes that could indicate advanced attacks or critical incidents.

To facilitate cybersecurity across large, complex distributed networks, Nozomi Networks Vantage provides SaaS-powered security and visibility for OT and IoT networks. It is an easy-to-deploy, easy-to-access solution that delivers the immediate awareness of cyber threats, risks and anomalies needed to respond faster and ensure operational resilience.

FIND OUT ABOUT VANTAGE

Nozomi Networks Vantage™ leverages the power and simplicity of SaaS to boost operational resilience across OT, IoT, and IT networks.

Find out why global industry leaders choose Nozomi Networks to secure their operational technology systems.

Request a Demo

See Customer Reviews

8. References

Executive Summary

1. **“Predicts 2021: Cybersecurity Program Management and IT Risk Management,”** S. Olyaei, K. Thielemann, R. Addiscott, K. Pratap, Gartner, January 8, 2021. (ID G00735901)
2. **“The Global Risks Report,”** World Economic Forum, January 15, 2020.
3. **“Ryuk ransomware responsible for one third of all ransomware attacks in 2020,”** Security Magazine, October 29, 2020.
4. **“2020 Unit 42 IoT Threat Report,”** Unit 42, Palo Alto Networks, March 2020.
5. **“H.R.1668 - IoT Cybersecurity Improvement Act of 2020,”** U.S. Congress, December 4, 2020.

   “IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain,” European Union Agency for Cybersecurity, November 9, 2020.

Threat Landscape

6. **“New action to combat ransomware ahead of U.S. elections,”** T. Burt, Microsoft, October 12, 2020.
7. **“Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,”** U.S. Department of the Treasury, October 1, 2020.
8. **"General Data Protection Regulation,"** European Parliament and the Council of the European Union, April 27, 2016.
9. **“Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities,”** National Security Agency, October 2020.
10. **“H.R.1668 - IoT Cybersecurity Improvement Act of 2020,”** U.S. Congress, December 4, 2020.
11. **“NIST Releases Second Draft of NISTIR 8259, ‘Recommendations for IoT Device Manufacturers,”** NIST, January 7, 2020.

    “IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain,” European Union Agency for Cybersecurity, November 9, 2020.
12. **"The U.S. Government is Creating Security Standards for IoT Devices,"** P. Bedwell, Nozomi Networks, December 2, 2020.
13. **“The Cyber Side of Vaccine Nationalism,”** D. P. Fidler, Council on Foreign Relations, September 14, 2020.

    “Inside hackers’ pivot to medical espionage,” Z. Dorfman, Axios, May 27, 2020.

    “Criminals and Nation-State Cyber Actors Conducting Widespread Pursuit of US Biological and COVID-19 Related Research,” FBI Cyber Division, May 21, 2020.

    “Breach Notification Portal,” U.S. Department of Health and Human Services.

    “2020-013 Ransomware targeting Australian aged care and healthcare sectors,” Australian Cyber Security Centre, August 2, 2020.
14. **“Alert (AA20-302A): Ransomware Activity Targeting the Healthcare and Public Health Sector,”** Cybersecurity and Infrastructure Security Agency, October 28, 2020.
15. **“The untold story of a cyberattack, a hospital and a dying woman,”** W. Ralston, WIRED, November 11, 2020.
16. **“Cyberattacks targeting health care must stop,”** T. Burt, Microsoft, November 13, 2020.
17. **“US charges Chinese Covid-19 research ‘cyber-spies,’”** BBC News, July 21, 2020.

    “Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research,” U.S. Department of Justice, July 21, 2020.

18. **"IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain,"** C. Zaboeva, M. Frydrych, Security Intelligence, December 3, 2020.

19. **"Statement by NCSC Director William Evanina: Election Threat Update for the American Public,"** Office of the Director of National Intelligence, August 7, 2020.

20. **"#PROTECT2020,"** Cybersecurity and Infrastructure Security Agency, 2020.

21. **"New cyberattacks targeting U.S. elections,"** T. Burt, Microsoft, September 10, 2020.

    "New action to combat ransomware ahead of U.S. elections," T. Burt, Microsoft, October 12, 2020.

22. **"Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees,"** Cybersecurity and Infrastructure Security Agency, November 12, 2020.

23. **"Developing Story: COVID-19 Used in Malicious Campaigns,"** Trend Micro, November 11, 2020.

    "CTI Investigation into COVID-19 Contact Tracing Apps," P. Ferguson, EclecticIQ, July 30, 2020.

    "Black Lives Matter Emails Deliver TrickBot Malware," T. Seals, Threatpost, June 11, 2020.

    "Cyberattacks targeting health care must stop," T. Burt, Microsoft, November 13, 2020.

    "Emotet Emails Strike Thousands of DNC Volunteers," L. O'Donnell, Threatpost, October 1, 2020.

24. **"MITRE ATT&CK® Matrix for Enterprise,"** MITRE, October 27, 2020.

    "ATT&CK® for Industrial Control Systems," MITRE, June 3, 2020.

25. **"Your Guide to the MITRE ATT&CK Framework for ICS,"** A. Di Pinto, Nozomi Networks, August 11, 2020.

Notable Threats

26. **"FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community,"** K. Mandia, FireEye, December 8, 2020.

    "FireEye Discovered SolarWinds Breach While Probing Own Hack," W. Turton, K. Mehrotra, Bloomberg, December 14, 2020.

    "Joint Statement by The Federal Bureau of Investigation (FBI), The Cybersecurity and Infrastructure Security Agency (CISA), The Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)," Cybersecurity and Infrastructure Security Agency, January 5, 2021.

27. **"Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise,"** Cybersecurity and Infrastructure Security Agency, December 13, 2020.

    "CISA Issues Emergency Directive to Mitigate the Compromise of SolarWinds Orion Network Management Products," Cybersecurity and Infrastructure Security Agency, December 14, 2020.

    "Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," Cybersecurity and Infrastructure Security Agency, January 7, 2021.

28. **"Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor,"** FireEye, December 13, 2020.

    "New Findings From Our Investigation of SUNBURST," S. Ramakrishna, SolarWinds, January 11, 2021.

29. **"SUNSPOT: An Implant in the Build Process,"** CrowdStrike, January 11, 2021.

30. **"Solarwinds Corporation Form 8-K,"** U.S. Securities and Exchange Commission, December 14, 2020.

31. **"Operation Quicksand: MuddyWater's Offensive Attack Against Israeli Organizations,"** ClearSky Cyber Security, 2020.

32. **“APT trends report Q3 2020,”** Global Research & Analysis Team, Kaspersky Lab, Securelist, November 3, 2020.

33. **“MontysThree: Industrial espionage with steganography and a Russian accent on both sides,”** D. Legezo, Securelist, October 8, 2020.

34. **“Attacks on industrial enterprises using RMS and TeamViewer: new data,”** V. Kopeystev, Kaspersky ICS CERT, Securelist, November 5, 2020.

35. **“Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware,”** NSA, FBI, August 2020.

36. **“Schneider Electric Security Bulletin: Trio Q and J Data Radios,”** Schneider Electric, November 10, 2020.

37. **“New action to combat ransomware ahead of U.S. elections,”** T. Burt, Microsoft, October 12, 2020.

    “An update on disruption of Trickbot,” T. Burt, Microsoft, October 20, 2020.

38. **“A Bazar of Tricks: Following Team9’s Development Cycles,”** D. Frank, M. Zhao, A. Dahan, Cybereason, July 16, 2020.

39. **"New Threat Intelligence Reveals Misuse of DNS Protocol,"** A. Di Pinto, Nozomi Networks, December 8, 2020.

40. **“A Bazar start: How one hospital thwarted a Ryuk ransomware outbreak,”** Red Canary, October 29, 2020.

41. **"Crime Laundering Primer: Inside Ryuk Crime (Crypto) Ledger & Risky Asian Crypto Traders,"** V. Kremez, B. Carter, Advanced Intelligence, January 7, 2021.

42. **“Anatomy of Attack: Inside BazarBackdoor to Ryuk Ransomware ‘one’ Group via Cobalt Strike,”** V. Kremez, Advanced Intelligence, November 6, 2020.

43. **“Ragnar Locker gang uses Facebook ads to pressure ransomware victim into paying,”** D. Riley, SiliconANGLE, November 10, 2020.

    “Ransomware Group Turns to Facebook Ads,” Krebs on Security, November 10, 2020.

    “Update Regarding Data Security Incident Due to Unauthorized Access,” H. Tsujimoto, Capcom, November 16, 2020.

44. **"Take a "NetWalk" on the Wild Side,"** McAfee, August 3, 2020.

45. **“Alert MI-000130-MW: Indicators Associated with Netwalker Ransomware,”** FBI, July 28, 2020.

46. **“Ransomware Alert: Pay2Key,”** Check Point Research, November 6, 2020.

47. **“Pay2Key – The Plot Thickens,”** Check Point Research, November 12, 2020.

48. **“Alert (AA20-280A): Emotet Malware,”** Cybersecurity and Infrastructure Security Agency, October 24, 2020.

49. **“SDBBot targeting health sector,”** Australian Cyber Security Centre, November 12, 2020.

50. **"Overcoming the Challenges of Detecting P2P Botnets on Your Network,"** A. Di Pinto, Nozomi Networks, October 13, 2020.

51. **“An Update for a Very Active DDos Botnet: Moobot,”** Netlab 360, July 9, 2020.

    “Multiple fiber routers are being compromised by botnets using 0-day,” Y. Ma, G. Ye, Lingming Tu, Y. Jin, Netlab 360, April 15, 2020.

    “Netlink GPON Router 1.0.11 - Remote Code Execution,” Exploit Database.

    “关于Moobot僵尸网口利用UNIXCCTV DVR在野0day漏洞的分析口告,” CNCERT, November 20, 2020.

52. **“Moobot vs. Gatebot: Cloudflare Automatically Blocks Botnet DDoS Attack Topping At 654 Gbps,”** O. Yoachimik, Cloudflare, September 16, 2020.

Vulnerability Landscape

53. **“ICS-CERT Advisories,”** Department of Homeland Security.

    “Common Weakness Enumeration,” MITRE.

54. **"CISA Alert: Sophisticated, Ongoing Cyberattacks Go Beyond SolarWinds,"** A. Carcano, Nozomi Networks, December 18, 2020.

55. **"Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families,"** N. Brubaker, D. Kapellmann Zafra, K. Lunden, K. Proska, C. Hildebrandt, FireEye, July 15, 2020.

    "Far-Reaching Third-Party Components Putting OT Networks At Risk," S. Brizinov, T. Keren, Claroty, September 8, 2020.

56. **"EKANS Ransomware and ICS Operations,"** Dragos, March 2, 2020.

57. **"ICS Advisory (ICSA-20-154-04): ABB Central Licensing System,"** Cybersecurity and Infrastructure Security Agency, June 2, 2020.

Notable Vulnerabilities

58. **"Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities,"** National Security Agency, October 2020.

59. **"Alert (AA20-283A): APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations,"** Cybersecurity and Infrastructure Agency, October 24, 2020.

60. **"Russian State-Sponsored Malicious Cyber Actors Exploit Known Vulnerability in Virtual Workspaces,"** National Security Agency, December 7, 2020.

    "Advisory ID: VMSA-2020-0027.2," VMware, December 3, 2020.

61. **"Netlogon Elevation of Privilege Vulnerability,"** Microsoft, August 11, 2020.

    "How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472," August 2020.

    "Alert (AA20-283A): APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations," Cybersecurity and Infrastructure Agency, October 24, 2020.

    "Attacks exploiting Netlogon vulnerability (CVE-2020-1472)," Microsoft, October 29, 2020.

62. **"Disclosure: Ripple20: 19 Zero-Day Vulnerabilities Amplified by the Supply Chain,"** JSOF, October 25, 2020.

63. **"The Aftershock of Ripple20,"** Finite State, October 12, 2020.

64. **"ICS Advisory (ICSA-20-343-01): Multiple Embedded TCP/IP Stacks,"** Cybersecurity and Infrastructure Security Agency, December 9, 2020.

    "Embedded TCP/IP stacks have memory corruption vulnerabilities: Vulnerability Note VU#815128," Carnegie Mellon University Software Engineering Institute, January 13, 2021.

65. **"Live off the Land? How About Bringing Your Own Island? An Overview of UNC1945,"** J. Moore, W. Ledzion, L. Rocha, A. Pisarczyk, D. Caban, S. Rincon, D. Susin, A. Monaca, FireEye, November 2, 2020.

    "In Wild Critical Buffer Overflow Vulnerability in Solaris Can Allow Remote Takeover — CVE-2020-14871," J. Thompson, FireEye, November 4, 2020.

    "Hackerhouse-opensource: exploits," Github, November 27, 2020.

66. **"CyberMDX Research Team Discovers Vulnerability in GE LightSpeed, Revolution, and other CT, MRI, and X-Ray imaging systems: CISA Advisory (ICSMA-20-343-01),"** CyberMDX, December 8, 2020.

    "ICS Medical Advisory (ICSMA-20-343-01): GE Healthcare Imaging and Ultrasound Products," Cybersecurity and Infrastructure Security Agency, December 8, 2020.

Recommendations

67. **"NSA & CISA Call For Action to Lower OT/IoT Cybersecurity Exposure,"** A. Carcano, Nozomi Networks, July 29, 2020.

    "Alert (AA20-205A): NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems," Cybersecurity and Infrastructure Security Agency, October 24, 2020.

    "Hardening Network Devices," National Security Agency, August 18, 2020.

    "Performing Out-of-Band Network Management," National Security Agency, September 17, 2020.

68. **“NIST Cybersecurity Practice Guide, Special Publication 1800-2: ‘Identity and Access Management for Electric Utilities,’”** National Cybersecurity Center of Excellence, July 2018.

69. **“Hackers hit Norsk Hydro with ransomware. The company responded with transparency,”** B. Briggs, Microsoft, December 16, 2019.

70. **“Best Practices for Securing Active Directory,”** Microsoft, May 31, 2017.

71. **“Remote Work After COVID-19,”** Human Resources Research Team, Gartner, July 16, 2020.

72. **“The Effect of the Coronavirus Pandemic on a Cybercrime Market: A Stimulation,”** A. V. Vu, Cambridge Cybercrime Centre, July 14, 2020.

73. **“Exploiting a crisis: How cybercriminals behaved during the outbreak,”** Microsoft 365 Defender Threat Intelligence Team, Microsoft, June 16, 2020.

“The Remote Access Genie is Out of the Bottle – Protect Your OT Systems,” P. Bedwell, Nozomi Networks, June 9, 2020.

74. **“BeyondCorp,”** Google Cloud.

“Zero Trust and its role in securing the new normal,” J. Lin, C. Hines, Microsoft, May 26, 2020.

75. **“Beating the Blockchain: Mapping Out Decentralized Namecoin and Emercoin Infrastructure,”** K. Perlow, Black Hat USA, August 8, 2018.

“How the Rise of Cryptocurrencies Is Shaping the Cyber Crime Landscape: Blockchain Infrastructure Use,” R. Eitzman, K. Goody, Jessa Valdez, FireEye, April 18, 2018.

76. **“OpenNIC Public Server,”** OpenNIC.

“Should OpenNIC drop support for NameCoin,” OpenNIC Wiki.

77. **“Hiding in Plain Sight: Part 2,”** J. Hammond, Huntress, August 20, 2020.

78. **“Attackers abuse Google DNS over HTTPS to download malware,”** A. Sharma, Bleeping Computer, September 2, 2020.

“DNS over HTTPS #DoH is definitely a thing. I think it will affect network security monitoring and detection in a non trivial way. #dailypcap,” @stvemillertime, Twitter, October 24, 2018.

“Waiting for goDoH,” L. Jacobs, Orange Cyberdefense. October 24, 2018.

“An Analysis of Godlua Backdoor,” Netlab 360, July 1, 2019.

“Three ways TLS 1.3 protects origin names,” P. McManus, Fastly, February 12, 2020.

79. **“A Bazar of Tricks: Following Team9’s Development Cycles,”** D. Frank, M. Zhao, A. Dahan, Cybereason, July 16, 2020.

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.

nozominetworks.com