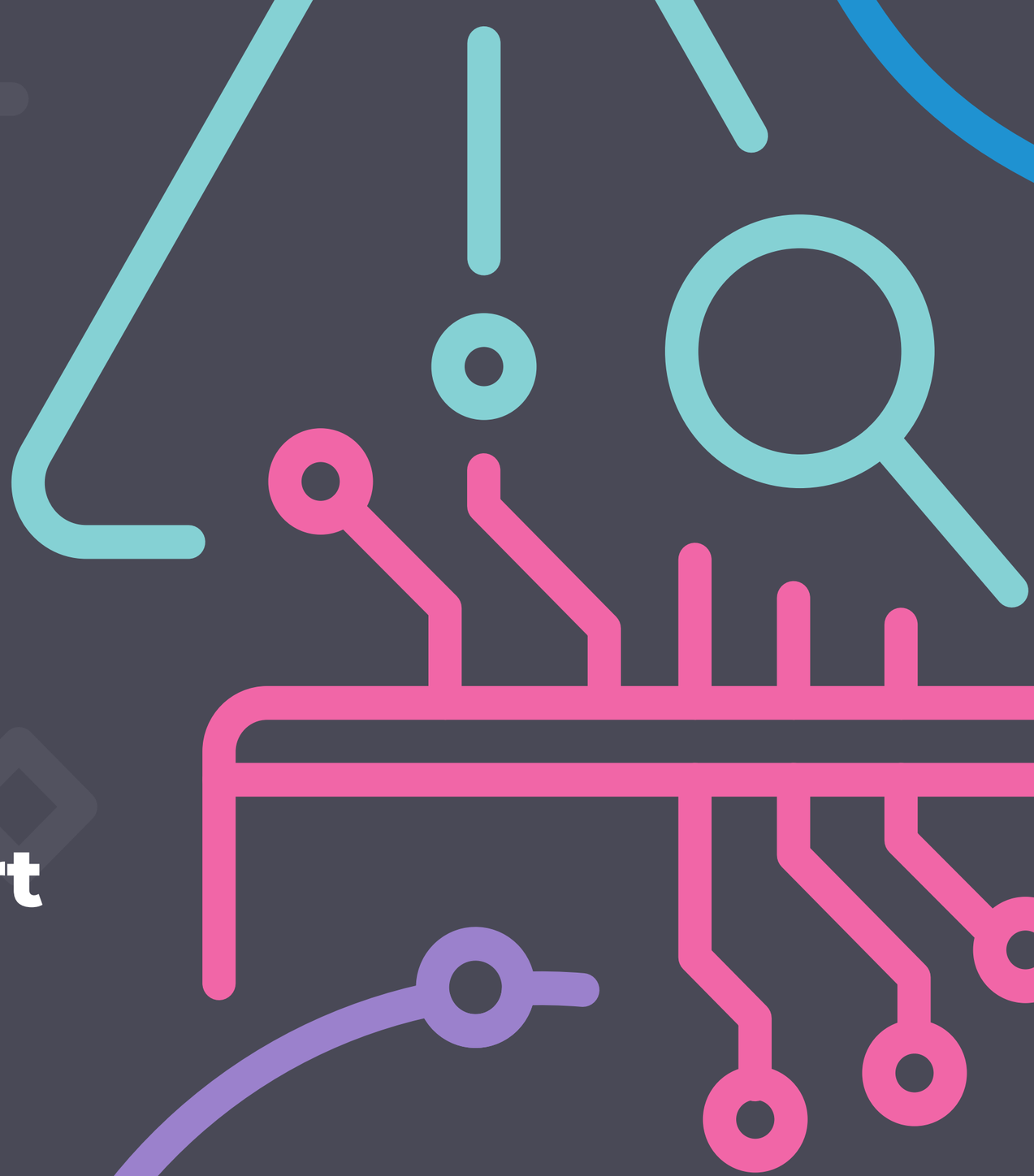
NOZOMI NETWORKS LABS

RESEARCH REPORT

OT/IoT Security Report

Trends and Countermeasures for Critical Infrastructure Attacks

2021 2H Review



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

Nozomi Networks Labs continues to aggregate industry trends and its own research in this semi-annual report covering the second half of 2021. Cybercrime continued to increase in the last six months of the year—ransomware and supply chain attacks dominated the headlines with the most impact and operational disruption. Despite renewed focus on the part of law enforcement, government bodies, and industry, the sophistication of the attack technology and risk to organizations continues to trend in the wrong direction.

To help security teams and researchers of OT/IoT environments, this report focuses on three main areas: trends in attacks, vulnerability research, and best practices in remediation efforts and technology. Some of the key focus areas include a deeper dive into ransomware attacks and Nozomi Networks' own research into vulnerabilities in security cameras and software supply chains. We also cover attack surface reduction, the role of Zero Trust in modern OT/IoT networks, and techniques for analyzing device firmware for vulnerabilities.

Ransomware Attacks Continue to Make Headlines and Cause Operational Disruption

Much like the first half of 2021, the second half of the year was filled with ransomware news and disruptions. It was reported that the Conti ransomware group extorted upwards of $150 million over the course of the year. Other prolific ransomware groups were active, with REvil targeting the software supply chain of IT solution provider Kaseya and BlackMatter—who many believe to be a successor to REvil—demanding a $5.9 million ransom from a U.S. farmer's cooperative.

Critical infrastructure sectors continued to be highly targeted, particularly transportation, healthcare and food. All are now perceived as high-value targets by ransomware groups as well as nation-state actors with geopolitical motives. Law enforcement organizations (LEO) also took significant actions against ransomware organizations and affiliates, often long-term operations involving the cooperation of many countries.

Not all the ransomware news was bad—leaked documents from a Conti group affiliate further confirmed researchers' understanding of tools and tactics used by ransomware gangs and helped shut down the group for a time. Nevertheless, affiliates usually migrate to other ransomware groups when one is compromised by law enforcement. This is the case with Conti, as affiliates were able to continue their attacks in 2021 2H against key industries.

KEY CRITICAL INFRASTRUCTURE INDUSTRIES TARGETED IN 2021 2H

- Transportation
- Healthcare
- Food

MOST NOTABLE VULNERABILITY – SECOND HALF OF 2021

Apache Log4j (CVE-2021-44228)

IMPACT

Many platforms and industries were widely affected. Ransomware gangs quickly designed repeatable attacks with a complete process for exploiting the vulnerability to encrypt files and extort payment. Organizations now realize the importance of maintaining a software bill of materials for their software applications so they can more quickly identify and remediate vulnerable systems.

The fallout from organizations not quickly remediating Log4j libraries could be felt for months or years to come.

Supply Chain Attacks Offer the Greatest Opportunity to Spread Damage Quickly

Supply chain attacks have the potential to disrupt hundreds or thousands of organizations, depending on how widely a common software component is used and the ease with which a vulnerability can be exploited.

The first widely reported supply chain attack was over a year ago when a SolarWinds vulnerability compromised dozens of critical network operations across industries and the federal government. Since then, we have seen growing concerns surrounding actual vulnerabilities and exploits in open-source code.

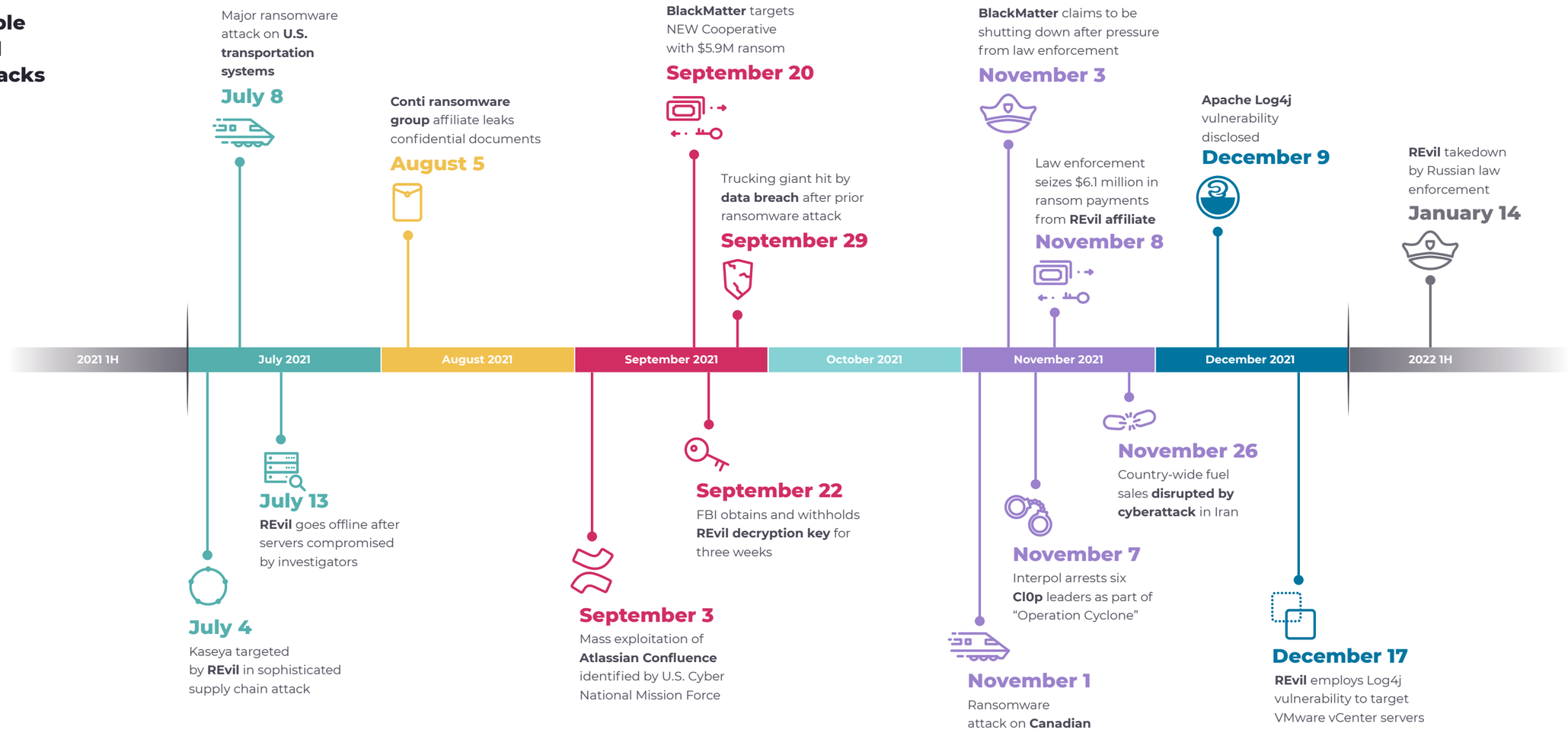
When vulnerabilities are announced in open-source software, which can be used by many applications, the damage can be just as, or even more, extensive than single-vendor software. It depends on how widely used the library component is.

This was the case with the December disclosure of the Log4Shell vulnerability. Log4Shell was found in the Apache Log4j (pronounced log-forge) open-source logging library, widely used in commercial applications and large online platforms.

Due to the simplicity of this exploit, attackers were quickly able to launch attacks ahead of remediation and patch efforts across the globe.

One of the largest ransomware groups was able to use the Log4j exploit within a week, launching an attack against VMware vCenter deployments.

Timeline of Notable Ransomware and Supply Chain Attacks in 2021 2H



Nozomi Networks Labs Vulnerability Research Focuses on OT/IoT Devices and Networks

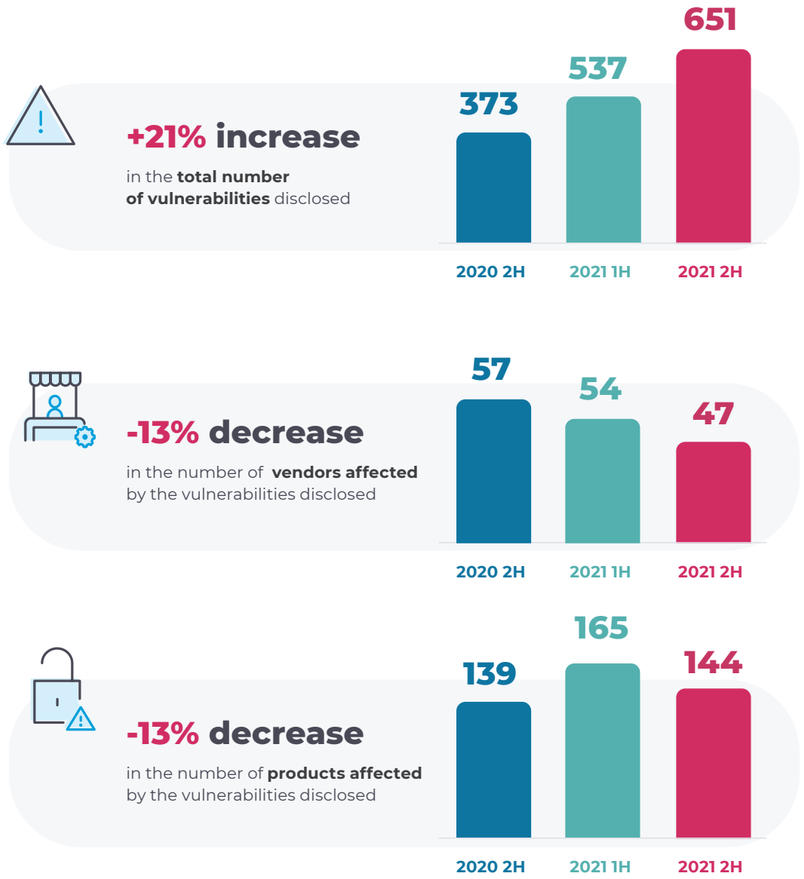
OT and IoT devices are the primary research area for Nozomi Networks Labs. In the last several years, IoT devices have become a common entry point to the entire network and are often overlooked compared to widely deployed IT platforms and operating systems.

IoT devices often run stripped-down operating systems with security features removed due to power and cost constraints.

While OT systems such as SCADA and ICS equipment could once rely on air gaps between Wi-Fi, the internet, and the larger IT cloud network, that is no longer the case. Security defenses need to be shored up accordingly.

In this semi-annual report, Nozomi Networks Labs highlights some of our key research areas, including vulnerabilities within supply chains, cloud platforms, and specific enterprise software platforms. In addition to reviewing some of the most impactful vulnerability disclosures made by the Labs team over the second half of 2021, we cover research regarding the attack surface of surveillance systems and what asset owners should keep in mind before deploying them within a network.

ICS Vulnerability Trends - 2021 1H vs. 2021 2H



Conclusions and Recommendations

Shoring up cyber defenses in OT and IoT environments requires a multi-pronged approach that often includes complementary technologies, well-defined oversight and processes, and necessary security hygiene. Too often, overburdened security teams allow human error to compromise even the most advanced defenses with weak passwords, misconfigured networks and devices, or social engineering. Many ransomware attacks begin with a naïve user clicking on a malicious email link in an otherwise well-defended network.

Network segmentation is another fundamental component of a cyberdefense strategy to prevent the spread of malware to critical applications and OT processes. Several technologies are useful to segment networks, such as VLANs and firewalls depending on the environment and policy requirements. In OT networks, the Purdue model is one way of creating network zones that align with process elements and system function.

However, too often we find organizations with completely flat networks (minimal segmentation), where easily compromised systems with mission-critical applications and processes have little or no isolation.

In this report, we make suggestions for increasing network segmentation, all the way to a Zero Trust model. Also known as microsegmentation, Zero Trust implies all network connectivity between individual endpoints is denied except those connections which are explicitly allowed. In migrating to a Zero Trust model, it is important to monitor traffic patterns to understand how legitimate traffic flows through the organization before specifying explicitly authorized connections to avoid disruptions.

We further discuss the importance of monitoring traffic to detect potential security threats, breaches, and other anomalies in both network flows and OT processes. Finally, we cover attack surface reduction and what can be effectively achieved with reasonable effort.

FOUR REMEDIATION MEASURES TO TAKE IMMEDIATELY

- Firmware Accessibility
- Network Monitoring
- Network Segmentation
- Attack Surface Reduction

By providing insights into key areas of the threat and vulnerability landscape, this report aims to help organizations assess and enhance their security posture.

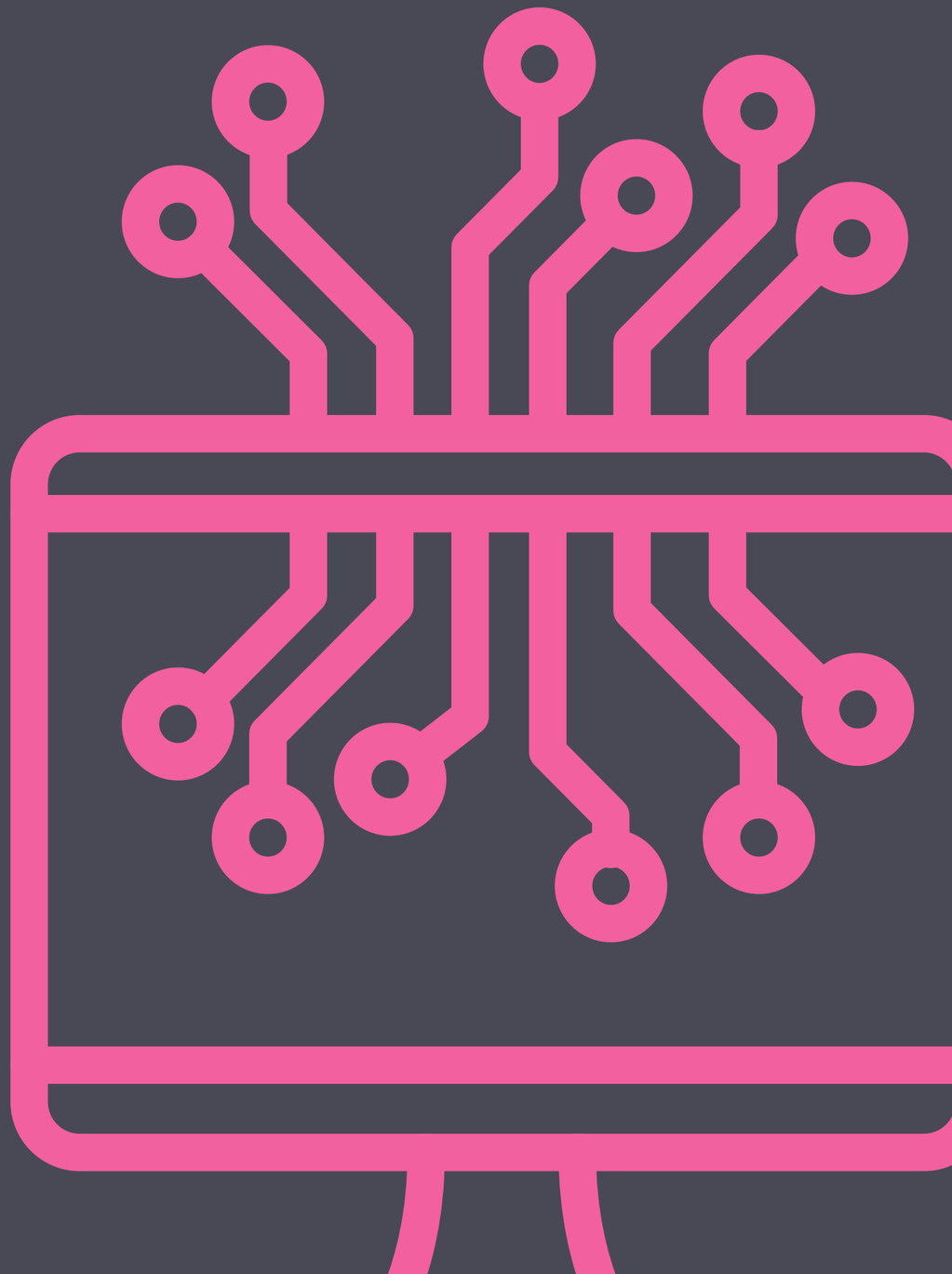
We encourage companies to move forward by improving OT/IoT visibility, security, and monitoring. With the sophistication and ruthlessness of today's adversaries, it is also important to adopt a post-breach mindset.

Continuous advancement of your IT/OT security posture is the best way to ensure the availability, safety, integrity and confidentiality of your operational systems.

NOZOMI NETWORKS LABS

2

The Threat Landscape



2.1 Notable Ransomware Updates

Ransomware captured a large share of cybersecurity headlines and continues to be top of mind for most organizations.

In 2021 2H we continued to see an increase in attacks and large ransom payments. But we are also developing more insight into the dynamics, tools and structure of ransomware gangs, along with renewed focus against them by international law enforcement organizations.

2.1.1 Conti Leak

The Conti ransomware group has been one of the most prolific Ransomware as a Service (RaaS) organizations since its first appearance in 2020. The group often targets hospitals and other first responder networks with substantial ransomware payments of over $1 million and is responsible for over 400 known cyberattacks. In 2021 alone, they're estimated to have extorted $150 million from victims.[1]

In August 2021, however, security researchers were presented with a trove of documents released by a disgruntled Conti affiliate.[2] The documents included affiliate manuals that described key tactics, techniques, and procedures (TTP), such as instructions detailing pre-attack reconnaissance, types of assets to target, which systems not to disable to avoid detection, and how to leverage Active Directory to help identify users with admin credentials.

The details contained in this document release provided researchers with insights to test and develop new mitigation techniques.

The maturity of these ransomware organizations—exemplified by the detailed "how-to" documentation and training for an extensive network of affiliates—was eye-opening to many.

Conti remains one of the largest, most sophisticated and ruthless ransomware organizations out there. In December, the group became the first ransomware organization to build a full attack chain around the Log4j vulnerability (**CVE-2021-44882**).[3] Within days of the initial disclosure, Conti affiliates were discussing how to exploit the vulnerability. Conti was able to put together a suite of tools and attack process. Within a week, affiliates began targeting VMware vCenter servers, one of many known systems that included the Log4j library and vulnerability. Researchers were surprised by how quickly a major ransomware gang took advantage of a new CVE to publish a set of tools and instructions to methodically penetrate new targets.

An important finding from the Conti leak was the common reliance of ransomware threat actors on Active Directory for lateral movement within the network using privileged credentials.

This should be a focus area for organizations to improve their defensive tactics, such as ensuring secure credentials and removing unnecessary privileged accounts.

2.1.2 Law Enforcement Actions Against Ransomware Groups

Recently the tables have turned on ransomware operators, with crackdowns from international law enforcement agencies leading to the shutdown of some of the largest ransomware gangs, including Cl0p, REvil and DarkSide. The arrests of six Cl0p leaders in Ukraine were the culmination of Interpol's "Operation Cyclone," a two-and-a-half-year effort to target the group.[4]

The FBI found itself in a difficult situation in September, when it held the decryption keys that could have unlocked hundreds of businesses affected by the REvil ransomware. The keys were obtained through access to the servers, but were not distributed to avoid tipping off REvil affiliates that were part of the dragnet. Victims included hospitals, schools and a range of commercial businesses that paid millions in ransom fees and other recovery costs.

In November, the BlackMatter group, responsible for the widely reported Colonial Pipeline attack under the name DarkSide, announced on its website that gang members were no longer available due to recent law enforcement efforts.[5]

There were rumors that BlackMatter was helping victims recover files, likely as part of a deal with law enforcement. Officers from Europol also arrested the Ukrainian group behind the MegaCortex, Dharma and LockerGoga ransomware.[6]

Governments are also going after the bitcoin exchanges that ransomware networks are using to launder payments into hard currency, in some cases revoking funds from digital wallets and accounts. The U.S. government recovered $6.1 million in extorted funds from REvil in November,[7] which is only a small portion of the over $200 million the ransomware group is estimated to have collected from operations.

In the same month, the U.S. Treasury Department also announced sanctions against at least two cryptocurrency exchanges, Chatex and Suex, which had facilitated malicious operators laundering payments from victims .[8] Despite the crackdown, many threat actors live comfortably in jurisdictions outside the reach of western law enforcement agencies.

The length of such investigations and the arrest operations are indicative of the complexity of taking down an entire ransomware network. If the large number of affiliates who execute most of the individual attacks are not removed, they will migrate to another ransomware service and continue their work. This is exactly what happened in the takedown of the REvil network as a result of a four-year operation.

In November, two Romanian nationals tied to the REvil ransomware gang were arrested, along with a suspect in Kuwait the same day.[9] The arrests followed a joint operation by international law enforcement agencies, including Europol and Interpol, that was able to intercept communications and seize infrastructure used during campaigns.

According to Europol, the REvil decryption tools have helped more than 1,400 companies decrypt their networks following ransomware attacks, saving over €475 million ($550 million) from being paid to cyber criminals.

In early December, Paul Nakasone, head of U.S. Cyber Command, confirmed that his agency, along with the FBI, NSA, and other federal agencies, had been taking direct concerted action to disrupt ransomware gangs and protect the critical infrastructure firms they had been targeting.[10]

As this report was going to production, news hit in mid-January 2022 that the Russian Federal Security Service (FSB) raided 25 residences suspected to be part of the REvil ransomware gang across Moscow, St. Petersburg, Leningrad, and the Lipetsk regions. Authorities seized more than 426 million rubles, $600,000, and €500,000 in cash, along with cryptocurrency wallets, computers, and 20 expensive cars.[11]

2.1.3 U.S. Food Sector Targeting

Ransomware groups REvil and DarkSide have made particularly devastating and publicized attacks in the U.S. against the agricultural and food sectors. In September, the FBI's Cyber Division released a summary of five major attacks against the industry in the prior year,[12] including JBS, a global food processor and meat supplier that paid an $11 million ransom to REvil.

The food and agriculture industries are designated as critical infrastructure sectors by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and are subject to greater oversight and assistance than other sectors. Because of the criticality of food production and delivery processes, hackers know that agriculture can be a very lucrative target. Farmers also have a difficult time taking production offline in the critical harvesting season and may be more compelled to come up with ransom funds.

In September, BlackMatter, who many believe to be a successor to REvil, attacked NEW Cooperative, an Iowa-based food distributor. NEW Cooperative refused to pay the $5.9 million ransom fee and opted to take their systems offline.[13] This is certainly an option for organizations with well-defined backup and remediation processes.

2.1.4 Hospital Targeting

Healthcare systems are currently seen as particularly susceptible targets due to their being overwhelmed by the COVID-19 pandemic, along with the life-threatening impacts of systems being down for an extended period. In August 2021, a ransomware attack on Scripps Health in California resulted in over $113 million in losses, according to the HIPAA Journal. This included $91.6 million in lost revenue over the four-week recovery period.[14] Several class-action suits are anticipated to increase the financial losses due to compromised patient data and litigation costs.

In October, CISA, the FBI, and the Department of Health and Human Services (HHS) issued a joint alert on ransomware activity targeting the healthcare and public health sector.[15] The alert detailed cyber threats using TrickBot and BazarLoader malware, which can lead to ransomware, data theft and disruption of healthcare services. The malware is distributed through phishing campaigns and malicious website links. Trickbot now includes a full suite of attack services such as cryptomining, credential harvesting, mail exfiltration and deployment of ransomware like Ryuk and Conti.

Another financially motivated group, FIN12, has been conducting widespread ransomware attacks, with at least 20% targeting the healthcare sector.[16] FIN12 also uses Trickbot to deploy Ryuk ransomware to target systems.

FIN12 stands in contrast to other ransomware groups such as BlackMatter who claimed they would not target hospitals and healthcare facilities, at least for the duration of the pandemic.

TRANSPORTATION INDUSTRY

186% increase
in weekly ransomware attacks between June 2020 and June 2021

2.1.5 Transportation System Targeting

In addition to the healthcare sector, cybercriminals have been ratcheting up their attacks on the transportation industry as a key component of a country's critical infrastructure. According to a Check Point study, the industry experienced a 186% increase in weekly ransomware attacks between June 2020 and June 2021.[17]

In July 2021, the Butte County (California) regional transit bus line systems were taken down over a weekend by an attack.[18] A Canadian transit system in Toronto was also hit by a ransomware attack at the end of October, but it did not cause any significant disruption to transit service.[19] A shipping company, Forward Air, experienced a data breach in September, following a ransomware attack at the end of 2020 which cost $7.5 million in lost revenue.[20]

In November, the Transportation Safety Authority (TSA) and Department of Homeland Security (DHS) issued two security directives for the rail transportation sector to implement an array of countermeasures to prevent disruption.[21] The security directives specified the need for a cybersecurity coordinator, incident reporting, and response plans, as well as ongoing vulnerability assessments consistent with NIST frameworks.

The TSA is now assessing threats to transportation and enforcing security-related regulations and requirements for rail transit owners/operators. The agency has similar national emergency powers with respect to maritime transportation, including port security. The TSA may soon seek to issue additional security directives to enhance cybersecurity efforts in maritime cargo shipping, navigation or communication, commercial fishing, and cruise lines.

2.2 Iran Fuel Subsidy Network Disruption

In October, Iran's petrol distribution network was targeted by an attack that disrupted the systems in charge of processing smart cards, which allow citizens to purchase fuel at subsidized prices.[22] There has been speculation regarding the group behind this operation, which disrupted fuel sales for several days.

What we want to emphasize about this attack are the tactics employed by the attackers, as every asset owner can benefit from understanding their aims.

A threat actor who wants to disrupt the availability of a region's fuel through a cyberattack has multiple options, ranging from interfering with OT operations in the refining process to preventing petrol stations from delivering the product. At the end of the day, what the attacker cares about is the outcome. If the weakest link in the chain is in the delivery process, that will likely be the target of the operation.

Asset owners should assess their posture with these threats in mind, taking a holistic approach towards all the processes required to keep the organization running. When Colonial Pipeline was hit by ransomware, what made the attack a success in terms of disruption was the company's inability to issue invoices and track the billing of its customers. A similar impact was created in Iran when citizens were blocked from buying fuel at an affordable price, triggering a series of social protests.

2.3 Threats to Building Automation: the Facebook Outage

Digital transformation has greatly increased the automation of many physical processes and systems. In the modern workplace, building automation systems (BAS) in offices are one of the most visible examples. These systems include everything from lighting and air-conditioning controls to building access systems and parking controls.

Cyberattacks against any large organization that reach the building automation systems can grind employee activity to a halt by disrupting any of the operational systems across the facility.

This became apparent in October when a server outage at Facebook disconnected data centers and network services from each other. The outage was not caused by a cyberattack, but by a flaw in the internal system that manages Facebook's global network backbone capacity.

Without the ability to access key applications, as well as the company's own DNS servers and other internet applications, many Facebook facilities were essentially offline. Employees reported the inability to enter buildings and conference rooms because badge readers and authorization systems were unreachable. The network outage complicated the remediation attempts of Facebook engineers even further, making it difficult to diagnose and remediate the issues, and to communicate with each other.

Facebook provided interesting commentary to this effect on its own post-mortem blog on October 5:

> We've done extensive work hardening our systems to prevent unauthorized access, and it was interesting to see how that hardening slowed us down as we tried to recover from an outage caused not by malicious activity, but an error of our own making. I believe a tradeoff like this is worth it — greatly increased day-to-day security vs. a slower recovery from a hopefully rare event like this. From here on out, our job is to strengthen our testing, drills, and overall resilience to make sure events like this happen as rarely as possible.
>
> **More details about the October 4 outage[23] - Santosh Janardhan, VP, Infrastructure, Meta**

2.4 Supply Chain Attacks

Supply chain attacks can be particularly disruptive because a single product or service can affect a large number of end user organizations.

One example is open-source software which can be used in many software products, if an open-source vulnerability can be identified and exploited. Understanding the software bill of materials (SBOM) of each vendor's product is becoming increasingly important for tracking, assessing, and managing vulnerabilities within an organization.

2.4.1 Kaseya

Kaseya is an IT solution provider with U.S. headquarters in Miami, providing unified remote monitoring, compliance, professional services automation, and network management. According to Kaseya, over 40,000 customers worldwide use at least one of their solutions, many of them MSPs and enterprise customers. Any supply chain attack against the company has the potential to spread throughout this installed base and do a tremendous amount of damage. In July, such a vulnerability surfaced.

Over the July 4th holiday weekend, Kaseya announced it was the victim of what would eventually be identified as a sophisticated ransomware attack[24] This particular attack, much like the SolarWinds attack at the end of 2020, targeted the software supply chain of the IT solution provider.

The supply chain ransomware attack was able to leverage an authentication bypass vulnerability in the Kaseya web interface. Attackers could circumvent the authentication, upload malware, and execute commands via an SQL injection. The breach was traced to 30 MSP customers very quickly. Because, like SolarWinds, the Kaseya software performed network management tasks, it had a high degree of trust in the target networks and could perform many malicious attacks.

Initially, it was difficult to assess the impact downstream to end users, but ultimately it was estimated that only several dozen customers had been directly affected and a couple thousand small businesses may have been affected down the supply chain. One coop supermarket chain in Sweden had to close for a time because they could not open their registers.

REvil's initial offer to Kaseya for a global decryption key was upwards of $50-70 million. Fortunately, by the end of July, Kaseya was able to take advantage of the compromise of the REvil decryption key by U.S. authorities. Kaseya also moved quickly to help customers take MSP servers offline and to patch the zero-day vulnerability, which greatly contributed to containing the downstream impact. Unfortunately, many end-user customers had already started negotiating or making ransom payments.

Remote monitoring and management systems will continue to be prime targets for supply chain attacks, which can deliver the keys to the kingdom in target networks over a large installed base.

Shortly after this attack, REvil servers were compromised by investigators and taken offline. However, the group has since resurfaced, possibly under other names, with new tactics and procedures.

2.4.2 Nation-state Actors Targeting IT Service Providers

The attack on Kaseya is just one example of a large, well-funded organization attacking a software vendor or IT service provider in the second half of 2021. Several other attacks took place, including nation-state actors targeting large service providers. The main motivation for these nation-state actors appears to be more espionage and intelligence gathering than purely financial profit from ransomware.

Nobelium, a Russian nation-state actor behind the SolarWinds attack in late 2020, started targeting resellers and service providers in May.[25] In October, Microsoft alerted over 600 customers that they had been targeted in these attacks, which didn't exploit vulnerabilities in any software but used phishing and password cracking techniques to compromise sites.

Currently, governments rely on private industry to provide much of the necessary security for critical infrastructure. Going forward, we can expect to see greater collaboration and oversight by the federal government in the U.S. with industry bodies, regulatory agencies, and critical infrastructure sectors like utilities and oil and gas industries.

We are already seeing efforts towards federal funding of cybersecurity defenses and greater information sharing across organizations as to the nature of emerging threats.

2.5 IoT Botnets

Botnets are networks of devices infected by malware and controlled by a single malicious party leveraging them for DDoS attacks or other malicious activities. In this section, we focus on three botnets that were prevalent in the last six months of 2021.

Meris botnet was relevant for the capacity of the attacks against Cloudflare and Yandex, Emotet returned to the fore after being taken down by global police action in January 2021 and a newly discovered malware leveraging the cross-platform capabilities of Go programming language targeted mainly network devices.

2.5.1 Meris

Meris is a botnet composed of infected routers and networking hardware mostly manufactured by MikroTik, a Latvian network equipment manufacturer. The vulnerability that was leveraged to exploit MikroTik's devices was discovered, published, and patched back in 2018 (**CVE-2018-14847**).[26] This critical vulnerability allows remote authenticated attackers to write arbitrary files on the device.

Meris attacked a Cloudflare customer in July with a 17.2 million request-per-second DDoS attack.[27] Since Cloudflare began tracking Meris in August, the botnet has executed an average of 104 DDoS attacks per day. In September 2021, the Meris botnet also attacked Yandex with 21.8 million requests per second, with the number of infected devices reaching 250,000.[28]

TARGET
Cloudflare Customer
REQUESTS PER SECOND
17.2 million

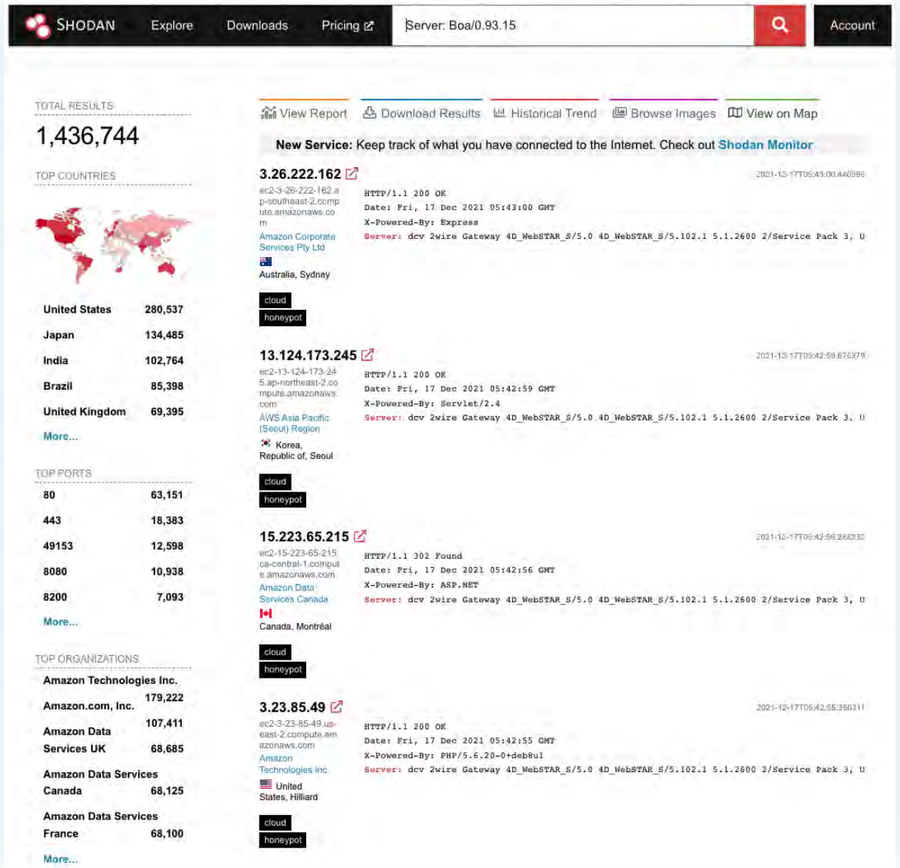
TARGET
Yandex
REQUESTS PER SECOND
21.8 million
INFECTED DEVICES
250,000

2.5.2 BotenaGo

BotenaGO is a new malware written in Go.[29] The threat actor behind the malware and infected devices is unclear but may be connected to the Mirai malware. According to AT&T analysis, the malicious software uses more than 30 exploits,[30] with CVEs issued from 2013 to 2020. Once installed on a vulnerable machine, BotenaGo receives instructions from the command and control (C&C) to infect other devices.

Most of the affected devices are network devices belonging to the following vendors: DrayTek, D-Link, Netgear, GPON, Linksys, XiongMai, Comtrend, Guangzhou, TOTOLINK, Tenda, ZyXEL, and ZTE.

One of the 30 exploits used by this malware targets Boa, a discontinued webserver used for embedded applications. A search for the targeted version of Boa in Shodan shows approximately 1.5 million exposed devices, which are thus potentially vulnerable and could be targets of a BotenaGo attack.



A search for the targeted version of Boa in Shodan shows approximately 1.5 million exposed devices.

2.5.3 Emotet

Emotet malware authors have used their malicious software to create a botnet of infected computers to use as infrastructure-as-a-service for other malicious actors. At the end of January 2021, Emotet was taken down by global police action.

After approximately 10 months, new Emotet activity has been detected: the first C&C after the shutdown was detected by feodo tracker on November 15th, 2021.[31]

At the time of writing there are 30 C&Cs online.[32]

2.6 Initial Access Brokers Markets

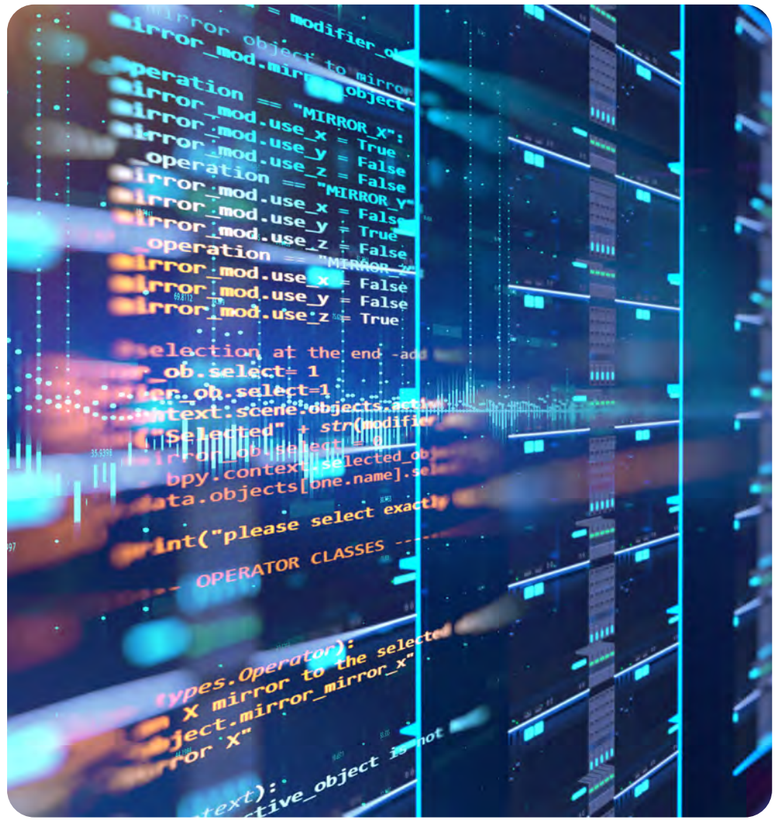
Initial Access Brokers are malicious actors that specialize in compromising organizations with any available technique. Entry points into companies are sold by these groups to other actors aiming to compromise the target even further and eventually deploy ransomware.

The price of the items being sold depends upon what level of access was achieved in the initial compromise, as well as which technology was used. There has been speculation in the past regarding the role of access brokers in major ransomware incidents, but the data available to justify the claims is often poor.

In August, security company Kela published an interesting analysis on Initial Access Brokers, documenting the recent trends in this market.[33] One of the most noteworthy takeaways of this research concerns the technology that provides remote access.

The fact that VPN credentials are still one of the most traded initial access mechanisms highlights how many organizations struggle to manage this aspect of their security posture.

Another interesting finding that emerged from Kela's research is a plausible correlation between a couple of listings affecting two different companies, and these two targets becoming victims of ransomware a few weeks later. While the data does not allow us to make a definitive conclusion regarding the causality of the events, we can still assume that many of the organizations listed in these markets don't have the means to detect unauthorized remote access.



NOZOMI NETWORKS

3

The Vulnerability Landscape

3.1 Analysis of ICS-CERT Advisories

In this chapter, we summarize all ICS-CERT vulnerabilities disclosed in 2021 2H, to help asset owners assess their posture in the OT and medical sectors.

We then discuss the latest vulnerability research trends, with a focus on those that have either been exploited by threat actors or have the potential to be used in future attacks.

Analyzing newly disclosed vulnerabilities or those being actively exploited by threat actors is important for a variety of reasons. First, it is important to understand if a given vulnerability belongs to an attack surface already known to security teams.

If that is the case, mature organizations can look at the problem with the knowledge that countermeasures are already in place. However, when a new attack surface is exposed through a new vulnerability, an organization's security posture must be reassessed.

Second, the existence of a vulnerability doesn't necessarily mean that a valid exploit is available to attackers in real-world scenarios. This is the main reason that the recent CISA initiative involving a catalog of known exploits[34] is particularly interesting. Since the vulnerabilities listed in the catalog are observed to have been exploited in the wild, asset owners can use this resource to prioritize their patching and mitigation efforts. A further refinement of this strategy would consist of categorizing these vulnerabilities based on the importance and location of the attack surface. Remote code execution on an internet-exposed VPN appliance should obviously be tackled before a privilege escalation on an isolated system, for example.

Finally, it is important to understand the latest trends in vulnerability research and associated exploitation because even though a technique might not be usable in a real attack today, it might still be used to compromise entire networks tomorrow.

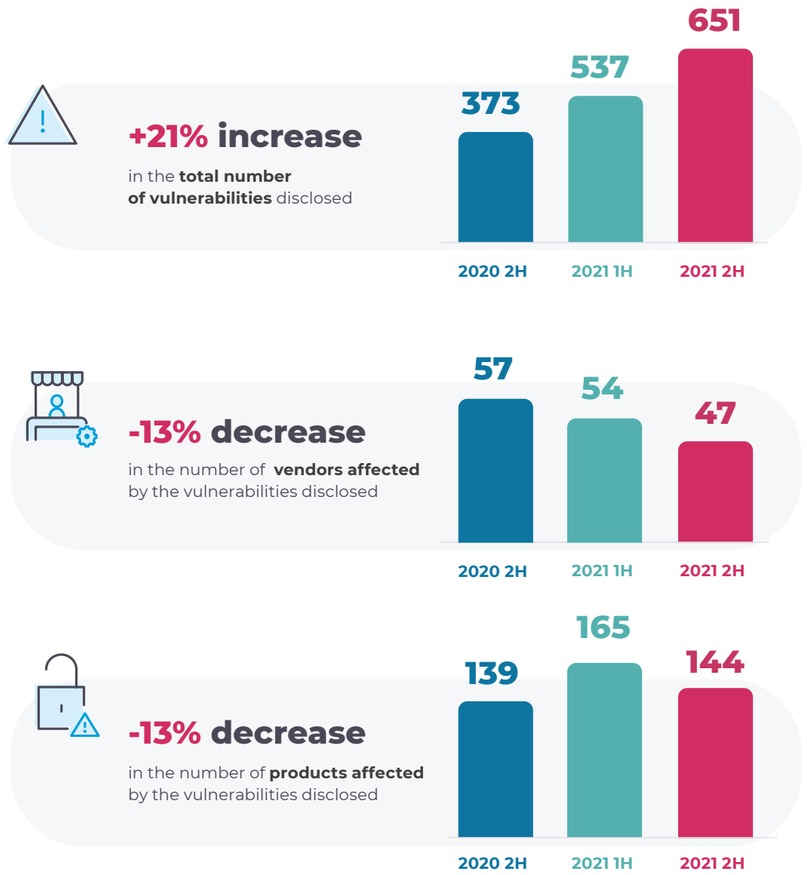
3.1.1 ICS Advisories

The second half of 2021 had continuous growth of the number of CVEs affecting ICS products, with a total of 651; a 21% increase over the first half of the year. This sharp increase in the number of vulnerabilities is not reflected in the number of products and vendors affected, which are instead moderately decreasing.

While the targets of security research analysis tend to vary over time, what's significant is that the number of CVEs is still climbing even after a strong 1H.

As we've mentioned in past reports, the security posture of many ICS software and hardware products lags behind what's commonly expected from modern IT systems. The technical difference between ICS and IT eventually comes to light when vulnerabilities are found in products that researchers had never previously targeted for in-depth assessments.

Between 2021 1H and 2H, there was a:

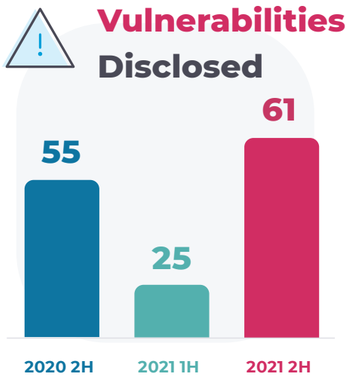


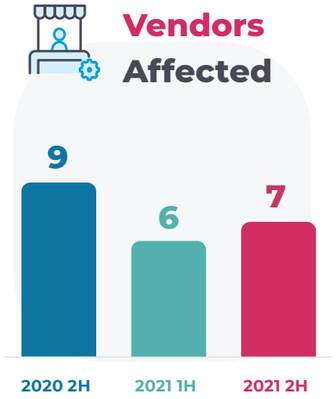
3.1.2 Medical Advisories

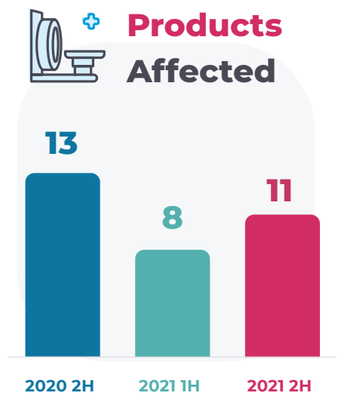
In our 2021 1H report, we described how the number of medical device vulnerabilities is heavily determined by researchers' access to the products, which leads to a low number of advisories that tend to pack a substantial number of vulnerabilities. In 2H, we also saw a vendor (Philips) proactively researching and disclosing a set of vulnerabilities affecting one of its products in ICSMA-21-187-01. This behavior should be praised by the community as it represents a sign of transparency and maturity.

This semester, two advisories containing vulnerabilities found by Nozomi Networks Labs were also published by ICS-CERT, ICSMA-21-322-01 and ICSMA-21-322-02. The first advisory concerned Philips Patient Information Center iX, the central application that receives and collects patient data. The second concerned the firmware of Philips devices that are often found in Philips PIC iX deployment. We invite readers to read through the related blog on patient monitoring systems, as it provides a breakdown of the attack surface exposed by the solution and corresponding vulnerabilities.

The low number of medical device vulnerabilities does not mean that these devices are inherently safer than other ICS devices—rather, it's more likely to indicate security researchers' limited access to medical devices.







NOZOMI NETWORKS BLOG

Five New Vulnerabilities Disclosed in Patient Monitoring Systems

To understand what attack surfaces are exposed by patient monitoring solutions, Nozomi Networks Labs configured a Philips Intellivue MX100 patient monitor connected to a PIC iX workstation.

We uncovered a set of five vulnerabilities, which ICS-CERT addresses in advisories ICSMA-21-322-01 and ICSMA-21-322-02.

Read More ›

3.2 Vulnerability Research and Exploitation Trends

3.2.1 Nozomi Networks Mitsubishi Research

In the last few months, ICS-CERT disclosed a series of vulnerabilities found by Nozomi Networks Labs affecting Mitsubishi Electric MELSEC iQ-R Series safety Programmable Logic Controllers (PLC). The set of vulnerabilities is the output of a research project on MELSOFT within Nozomi Networks Labs. It is particularly interesting because it exposes security issues concerning an attack surface which was not explored in this family of controllers.

Mitsubishi safety PLCs, as opposed to non-safety controllers, have full authentication to prevent unauthenticated operators from performing safety-sensitive operations. When chained together, these vulnerabilities allow for novel attacks to be performed against iQ-R PLCs. The vendor has released a series of mitigations that asset owners should follow to minimize the risk of compromise.

One of the most interesting takeaways from this research is that the authentication bolt-on to OT protocols sometimes does not present the same level of security asset owners might expect. Network monitoring is one of the main building blocks for a defensive strategy, since it allows detection of the exploits against these vulnerabilities, in addition to keeping track of the actions of regular operators.

3.2.2 Nozomi Networks IoT Security Camera Research

Nozomi Networks Labs recently published a white paper providing asset owners with a compendium of all the security aspects that should be considered when evaluating an IP video surveillance solution. Considering how pervasive these devices are within any organization, from security cameras

NOZOMI NETWORKS BLOG

New Research Uncovers 5 Vulnerabilities in Mitsubishi Safety PLCs

Nozomi Networks Labs has discovered five vulnerabilities affecting Mitsubishi safety PLCs that relate to the authentication implementation of the MELSOFT communication protocol.

We caution asset owners to be aware of the technical details and failure models of OT protocols, and not rely too much on the security of their authentication.

Read More ›

to access controllers, particular attention should be paid to the selection process.

When selecting a surveillance system, an often-overlooked element is the ability to obtain unobstructed access to the firmware of the devices deployed. Some vendors try to justify this choice by stating that the effort is security driven. We argue instead that the security posture of a network is threatened by this design.

A companion issue for asset owners is the ability to inspect the device while in use and evaluate its security posture. While most of the components of a video surveillance solution tend to have a remote access capability that is often switched off by the vendor, there are entire categories of devices found in an enterprise network that don't.

A good rule of thumb that can help asset owners decide when it would be acceptable to deploy a non-inspectable device is to determine its precise position within a network. A PLC that is deployed in a segmented network and is carefully monitored can constitute an acceptable risk. A VPN appliance that is exposed to the internet and is responsible for connecting remote endpoints to the internal network of an organization has a different risk profile. In a recently published "Selecting and Hardening Remote Access VPN Solutions" document, NSA and CISA clearly state that not having full inspection capabilities into a VPN device effectively compromises any investigation into sophisticated malicious actors' activity.[35]

Devices belonging to a video surveillance solution represent a strategic target for threat actors seeking persistence within a network. Network monitoring is a baseline tool that gives security teams visibility into the interactions of malicious operators with compromised targets.

Having the capabilities to inspect a device is a logical complementary approach in a mature security program.

3.2.3 Supply Chain Vulnerabilities

In 2021 2H, the general understanding of the danger posed by supply chain vulnerabilities is maturing. The term 'supply chain vulnerability' is broad, describing many situations. For instance, several supply chain vulnerabilities are caused by the malicious modification of libraries in the official languages' repositories, such as npm for JavaScript sources and PyPi for Python libraries. The most notable vulnerability of the last six months affected Log4j, an Apache open-source Java library used for logging, which impacted most of the companies using Java.

It's challenging for companies to have a complete inventory or at least have situational awareness of the libraries their software depends on, but it is key to define a strategy that would allow proper visibility into the software stacks.

3.2.3.1 npm Packages (coa, uaparser.js, noblox.js)

Between October and November, multiple JavaScript libraries in the official npm repository were modified by the addition of malicious code responsible for stealing passwords and mining cryptocurrencies. Maintainers' accounts of rc package (a configuration loader), coa package (a command line argument parser)[36] and UAParser.js (a library to retrieve information from User-Agent data)[37] were compromised, allowing the malicious actor to access and publish the compromised versions. Even though these very popular libraries have not been maintained for years (since at least 2018 for coa and 2015 for rc), they are widely used and have millions of weekly downloads. Shortly after the discovery, the npm security team quickly removed all compromised packages.

Noblox.js a slightly less popular JavaScript package (with approximately 20,000 weekly downloads) and was infected with the same objective of stealing passwords, installing

remote access trojans on the victims' computer, and deploying ransomware. In this case, the malicious actor created typosquatting packages mimicking the legitimate noblox.js.[38]

3.2.3.2 PyPi Packages

In November, eight libraries containing malicious code were removed from PyPi, the official repository for Python components. Some of these infected libraries allowed an attacker to connect to a server and execute any malicious code provided by the server on the infected device. In other cases, the libraries contained malicious code that would steal general system information, Discord tokens and payment card information saved in the victims' browsers.[39] In the last few years, PyPi has been a target of this type of attack, mostly using a typosquatting attack on very commonly used packages. PyPI has removed the affected packages they have found, but there is still the possibility of similar attacks occurring in the future.

3.2.3.3 GoCD

GoCD is a popular Continuous Integration and Continuous Delivery (CI/CD) solution. It is usually strategically placed where it can access production environment and private source code repositories to automate build and release processes. Because of its nature and strategic position in the networks, this type of device is usually an attractive target for malicious actors.

At the end of October 2021, GoCD released a security update to address a critical authentication vulnerability which allows attackers to take over the underlying server, access the API key for external code repositories, and access and modify the files that are being produced as part of the build process, leading to supply chain attacks.[40] This vulnerability has already been fixed; we therefore recommend upgrading to the latest version of GoCD.

3.2.3.4 Log4j

In December 2021, security researchers discovered a remote code execution vulnerability in Log4j, a very common Java library used for logging.

The vulnerability, eventually dubbed "Log4Shell" and tracked with **CVE-2021-44228**, affects a wide range of Log4j versions which, coupled with the library's popularity and relative ease of exploitation, produced a perfect storm scenario for many security teams.

Two additional vulnerabilities, **CVE-2021-45046** and **CVE-2021-45105**, were later disclosed. Their impact was limited as they required a non-standard configuration to be used, in addition to the latter vulnerability being only a denial of service.

At a high level, the exploitation of Log4Shell consists of submitting a malicious string that is eventually consumed by the vulnerable library, which will finally load the attacker-supplied code. Since a working public

proof-of-concept was immediately available, malicious actors started scanning internet-reachable systems to compromise public-facing services.

The first problem for security teams is identifying vulnerable Log4j instances within their organization's systems. Since a comprehensive software bill of materials (SBOM) for third-party software is rarely available, this is by no means a small feat, given the number of systems typically deployed. As Java libraries are easy to identify even in their binary form, several tools and scripts are available to blue teams to automate this initial task.

Once a software stack running Log4j is identified, a mitigation strategy should be devised if patching is not yet an option. In both cases, security teams should leverage the available tools, such as network monitoring platforms, to find evidence of malicious actors' activity. Given the specific requirements for the exploitation of Log4Shell, there are several leads that can be used to track attackers.

While the most exposed attack surfaces that were vulnerable to Log4Shell have likely been patched, in the next few months we might experience a long tail of attacks leveraging this vulnerability, for instance to achieve lateral movement within an already compromised network. For this very reason, it is important that a comprehensive exposure audit is performed to identify plausible entry points.

Overall, Log4j has once again highlighted the need for a detailed software inventory that can provide security teams a top-down view of the different software stacks running within an organization. SBOMs can be a first step in this direction, but their success will depend on widespread adoption by software providers, among others.

NOZOMI NETWORKS BLOG

Critical Log4Shell (Apache Log4j) Zero-Day Attack Analysis

Nozomi Networks set up a honeypot to monitor the Apache Log4j vulnerability, and provides technical details related to how malware authors immediately took advantage of this vulnerability.

This blog explains the Log4Shell attack surface and shares an example of a full infection chain associated with the Muhstik botnet.

Read More ›

3.2.4 On-premises Solutions

Many services offer both cloud and on-premises solutions; the latter is sometimes preferred by companies because it is located within the organization, and operations and maintenance are managed completely internally. One of the main security concerns for on-premises solutions is that it is typically easy to find misconfigured and unpatched systems exposed on the internet.

In the last six months, GitLab and Confluence have been targets of attacks leading to Remote Code Execution. Even months after these vulnerabilities have been published and fixed by the vendors, there are still many vulnerable instances on the internet.

3.2.4.1 Confluence RCE

In September 2021 the U.S. Cyber National Mission Force issue an alert regarding an ongoing mass exploitation of Atlassian Confluence.[42] Confluence is a collaborative wiki service used for enterprise documentation. Some of the users deploy the software on-premises, but most run their own managed services.

The exploited vulnerability found on Confluence Server and Data Center allows an unauthenticated attacker to execute arbitrary code on the server. Thousands of Confluence instances exposed on the internet seem to run a vulnerable software version. Censys found more than 14,000 services self-identifying as Confluence servers, of which approximately 13,000 ports and 13,000 hosts were running an exploitable version of the software.[42]

CENSYS IDENTIFIED:

14,701 services
that self-identify as Confluence servers, and of those,

13,596 ports and

12,876 individual IPv4 hosts
are running an exploitable version of the software.

3.2.4.2 Gitlab RCE

Many public GitLab instances were exploited due to an improper validation of images that lead to Remote Code Execution. The hacked GitLab instances were found to be part of a botnet used for large scale DDoS attacks.[43] This vulnerability identified with CVE-2021-22205 was patched in April 2021, but in November 2021, Rapid7 stated in a blog post that out of the 60,000 GitLab instances facing the internet only 21% of them had been fully patched, while at least 50% of them are still vulnerable.[44]

3.2.5 Kubernetes-based Bruteforce Campaign

In July a Joint Cybersecurity Advisory from U.S. and UK agencies described a global bruteforce campaign performed by Russia's GRU that aimed to compromise enterprise and cloud environments.[45] This campaign presents a series of characteristics that make it stand out.

The most unique feature is the usage of a Kubernetes cluster to coordinate a series of worker nodes that perform the actual bruteforce. The released data allows us to understand how the worker nodes were distributed geographically. It's the first time that a bruteforce campaign with this level of engineering sophistication has been publicly disclosed.

A further interesting characteristic of this campaign concerns the selection of the targets, which range from government and military organizations to logistic companies and think tanks, mostly based in the U.S. and Europe.

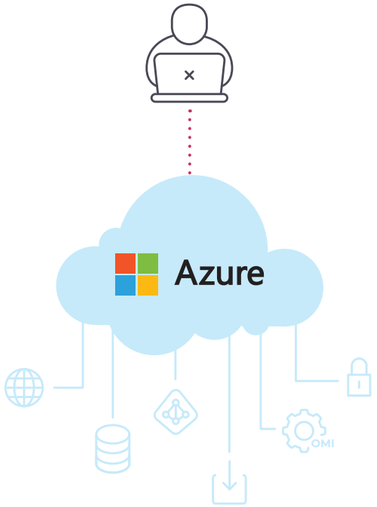
Finally, the threat actor has been targeting a variety of protocols with the aforementioned setup, such as HTTP(S), IMAP(S), POP3 and NTLM. Once a set of credentials was discovered to be working with a given service, the attackers were

also found to be deploying the usual lateral movement techniques within the compromised organization.

Bruteforce has always been noisy from a detection point of view, and this campaign, notwithstanding its sophistication, is no different. Defenders have several detection data points, beginning with an analysis of the amount of failed authentication attempts. The best countermeasure, though, is to deploy authentication features that can neuter the possibility of having credentials bruteforced, such as multi-factor authentication and time-outs.

3.2.6 Cloud Services

The rapid shift to cloud services has made them a precious target for malicious actors. Many security researchers are testing cloud platforms and responsibly disclosing the vulnerabilities to improve the security of these systems. In the last year we have seen many vulnerabilities in major cloud providers and in H2 we have seen researchers focusing mostly on the Azure cloud platform.



3.2.6.1 ChaosDB

ChaosDB is a critical vulnerability in the Azure cloud platform that allows a user to gain admin access to another Azure user's resources, impacting thousands of Azure customers. ChaosDB is based on multiple misconfigurations of the Jupyter Notebook container of Azure Cosmos DB.[46] Jupyter Notebook, a feature of Cosmos DB, is an open-source web application where users can create and share documents containing code, equations, visualizations and narrative text used by data scientists and developers.

The first misconfiguration is a Local Privilege Escalation on Jupyter Notebook that allows root privileges to be obtained in the container. As a second step, the researchers obtained Unrestricted Network Access which granted access to all the Cosmos DB instances in the regional cluster. Moreover, once in possession of the certificate, access can be maintained over the internet. ChaosDB was reported by Wiz researchers in August 2021 and Microsoft disabled the vulnerable feature shortly thereafter, but it is not yet clear if the vulnerability has been exploited in the wild.

3.2.6.2 OMIGOD

All Azure customers on Linux machines are at risk of potential exploitation due to another vulnerability affecting Azure's Open Management Infrastructure (OMI), a service for managing distributed systems. Whenever an Azure user creates a Linux VM and enables a list of services such as Azure Automation, Azure Automatic Update, Azure Operations Management Suite, Azure Log Analytics, Azure Configuration Management, Azure Diagnostics (and possibly more), OMI is also automatically installed on the system. OMIGOD is the name assigned to a collection of four vulnerabilities with a high CVSS score, allowing Remote Code Execution and Local Privilege Escalation.[47]

The OMIGOD vulnerability is exploited by simply skipping the authentication request and thus gaining root access on the system. Given its nature—collecting statistics and syncing configurations—the OMI agent is accessible from the internet, leaving the system vulnerable to any remote attacker. This type of vulnerability is very often exploited by botnet operators. As stated by McAfee, the Mirai botnet was actively scanning for OMIGOD vulnerabilities, and in case of successful compromise they closed port 5896 to prevent any other attacker from exploiting the same machine.[48]

3.2.6.3 Azurescape

Azurescape is yet another Azure vulnerability; it was reported by Unit42 Palo Alto researchers in September.[49] This vulnerability affects Azure Container instances, Azure's Container-as-a-Service solution which allows users to run containers without managing the underlying systems, as well as containers in the Azure Virtual Network. Azurescape allows a malicious Azure user to break out of their container and execute code on environments belonging to other users, leading to account takeover. Azurescape is a three-step attack leveraging, among others, a two-year-old vulnerability (**CVE-2019-5736**) which allows the container environment to be broken out from.

Shortly after researchers reported the vulnerability, Microsoft released a patch for ACI. There is no evidence of Azurescape being exploited in the wild, but we highly recommend checking access logs for suspicious activities.

3.2.7 Enterprise Software

Our previous security reports have emphasized how often the security posture of software commonly found in the enterprise world is not as solid as that of other software that is generally more exposed to attackers, such as a modern browser. Threat actors are obviously aware of this situation and are improving their target selection, based on this insight. In 2021 2H, there were two specific instances where this very scenario recurred: SolarWinds' Serv-U SSH and Palo Alto's GlobalProtect Firewall/VPN.

3.2.7.1 SolarWinds Serv-U SSH

In September Microsoft disclosed a vulnerability on the SSH component of SolarWinds Serv-U FTP software.[50] Based on gathered data, the vulnerability was exploited by a threat actor operating out of China, but crucially the company didn't capture the actual exploit.

With only the knowledge of the attack surface under attack, a team of Microsoft researchers set off to build a fuzzer that would focus on the pre-authentication code of the SSH implementation. Eventually, the vulnerability was found, but what became evident is how vulnerabilities in the SolarWinds software made exploitation easier for the threat actor. Specifically, two DLLs loaded in the target process had Address Space Layout Randomization (ASLR) support disabled. This is quite unheard of for a network service in modern stacks, as it allows attackers to easily exploit the vulnerability.

3.2.7.2 Palo Alto GlobalProtect Firewall/VPN

In November, security company Randori disclosed a remotely exploitable vulnerability affecting Palo Alto GlobalProtect Portal VPN.[51] The interesting fact about this disclosure is that in the virtualized version of GlobalProtect, the ASLR was found to be disabled. This is particularly worrisome as the VPN portal is often exposed over the internet. Randori has also developed a working proof of concept for the virtualized product to demonstrate the feasibility of the exploitation.

In both the cases discussed in this section, the lack of ALSR was the main element that raised concerns over the quality of the products discussed. Assessing the security posture of complex products, though, is not limited to a checklist of the exploit mitigation in place, as advanced attackers might be able to bypass those. It is also important, for instance, to understand how a compromise of a given target can be detected, and this often translates to being able to observe and inspect the product.

4

Remediation

4.1 Suggested Remediation Strategies

Improving network reconnaissance and monitoring with an understanding of normal process activity can help quickly identify potential threats and correlate anomalies to prioritize alerts and remediate efforts more efficiently. A multi-pronged approach to cybersecurity, including knowing what devices are on your network, what versions of software and third-party libraries they are running with known vulnerabilities, and who or what they are communicating with, is going to be key to staying ahead of emerging threats in 2022 and beyond.

Some of the suggestions that we make in this chapter include deploying network segmentation to contain the spread of malware and considering a Zero Trust philosophy to limit malicious activity in a more connected world. Organizations should also be looking to reduce the attack surface available to attackers by removing known vulnerabilities, as well as seldom-used services and applications.

4.1.1 Firmware Accessibility and Device Introspection

By firmware accessibility, we refer to the ability to analyze the binary images running on devices without needing to break any mechanism put in place by the vendor. This accessibility is important because it allows security teams to independently gather information about the software stack, which is not exposed in network traffic. The data that can be extracted concerns either the specific software components installed, or the configuration statically set by the vendor.

Device introspection concerns the possibility of inspecting the status of a device at runtime. The concept of introspection can take several forms depending on the object of the analysis, from a simple filesystem listing to a more sophisticated analysis of kernel data structures. The general idea is that by performing the measurements, defenders can gather metrics that can be useful to derive the security status of a device.

Obviously not all devices deployed within a network were designed with introspection in mind. We suggest asset owners perform a survey and gather a clear understanding of devices that are not accessible. This list should then be supported with an assessment that broadly describes the likelihood of a given device being exploited. For instance, an IoT camera is more likely than a PLC to be directly leveraged as a launch pad by an attacker.

From a security point of view, one of worst situations for any organization is to have a sophisticated attacker performing its malicious activities from a completely

locked down device, inaccessible to the security team. Network monitoring is the only tool that can help at least isolate the compromised device and more broadly understand the activity of a malicious actor.

4.1.2 Network Monitoring

Advanced malware threats designed to disrupt industrial processes typically go through lengthy infection, reconnaissance, and lateral movement phases before executing their material objective.

An important part of neutralizing threats before they can disrupt any processes involves early warning across all three phases of attack. Proper network monitoring alerts you about early-stage infection and reconnaissance and provides information that helps any stage of remediation, including the post-mortem to identify what the attackers did.

- In **Phase I**, anomaly detection can identify malware that is beaconing out to an external Command and Control server (C&C) through its connections to a new public IP address. Using Yara rules, a built-in analysis toolkit can immediately identify specific files associated with the malware. Assertions can also be used to detect data and events in network traffic related to the presence of the malware at a particular site.
- In **Phase 2**, before attacking, malware frequently performs a low-level reconnaissance of valuable network resources and vulnerabilities. During this phase, anomaly detection can identify new commands in the host network and generate 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.
- In **Phase 3**, if an attack occurs, it is quickly identified, and an alert is sent out. This enables you to implement new firewall rules or take other actions to stop further attack commands.

With integration to multiple firewalls, monitoring can go beyond detection to tackle prevention, by automatically triggering the implementation of rules that block an attack upon detection of irregular commands.

4.1.3 Network Segmentation

Nearly all forms of malware, including ransomware, rely on network connectivity to move laterally throughout the network, and to identify and compromise other systems. Network segmentation is a fundamental tactic that can inhibit the spread of malware or any unauthorized traffic within the internal network. Typically, network segments or zones have security checks to move between zones, allowing legitimate users and traffic through to appropriate destinations, while containing threats to a small, potentially safe, area within the larger network.

An example of network segmentation being used to block unauthorized traffic would be a company's DMZ separating the public internet from the internal corporate network and web applications, a guest network, or Purdue model zones within an industrial control environment. Technologies that can segment the network include virtual LANs (VLAN), firewalls, network bridges, overlay networks, and more.

If segmentation is an effective way to stop malware propagation, then the ultimate in segmentation is microsegmentation, which is gaining traction as a strategy to stop the spread of malware completely. Going by the more common name of Zero Trust, the goal is to assume that no traffic can move throughout the network except that which is explicitly allowed by defined network and security policies. The term microsegmentation arises from the end goal of every single device having its own segment, with its own access and security policies.

Zero Trust has been encouraged by government agencies and security experts for critical infrastructure for some time. The challenge has been that increasing the restraints on malware also increases the complexity of defining and implementing legitimate traffic flows. This can easily

increase the likelihood of policy errors that could break user and application access, and complicate network security administration. Zero Trust does not come at zero cost.

Still, many operational technology (OT) networks that relied on being air-gapped from the rest of the corporate network are lacking any segmentation at all, or a limited form of segmentation based on a design such as a Purdue model. Starting from a wide-open, or flat network, and jumping all the way to Zero Trust can be quite daunting for most organizations already stressed with limited resources.

A reasonable segmentation strategy, with varying controls at key choke points is an important and cost-effective way to start. Coupled with ongoing traffic monitoring and comparing actual traffic patterns to desired Zero Trust policies before introducing rigid controls can allow organizations to incrementally approach Zero Trust segmentation as time and resources allow.

4.1.3 Attack Surface Reduction

An attack surface is the portion of a system or network accessible to potential attackers. The larger the attack surface, the more potential for vulnerabilities and administrative errors that can pave the way for initial penetration and a more extensive attack on the network. Complexity of system, network, and process design is often the root cause of cyberattacks, as well as the source of human error and higher administrative costs.

To reduce attack surfaces, organizations should follow a few key recommendations:

- *Zero Trust and network segmentation* – As mentioned above, Zero Trust models or further network segmentation effectively reduce the attack surface that is exposed to potential intruders. You are effectively reducing the number of accessible systems and services available from any other device or user on the network.
- *Effective asset and vulnerability management* – Tracking available devices and continuously managing known vulnerabilities (with remediation efforts) will reduce the available attack vectors. Rogue devices installed by a shadow IT organization also need to be identified and eliminated or moved to be a tracked and managed device for policy and compliance purposes.
- *Training and audit procedures* – To reduce human error, such as poor password management, proactive attention to best practices, with corresponding process audits, should be considered. Simplifying the number of points of remote access, the number of users accessing required systems, and removal of seldom-used services and applications all serve to reduce complexity and associated attack services.

5. References

[1] Lisa Vaas, **"Conti Ransomware Gang Has Full Log4Shell Attack Chain,"** *Threatpost*, December 20, 2021.

[2] Lawrence Abrams, **"Angry Conti Ransomware Affiliate Leaks Gang's Attack Playbook,"** *BleepingComputer*, August 5, 2021.

[3] Lisa Vaas, **"Conti Ransomware Gang Has Full Log4Shell Attack Chain,"** *Threatpost*, December 20, 2021.

[4] Lawrence Abrams, **"Operation Cyclone Deals Blow to Clop Ransomware Operation,"** *BleepingComputer*, November 7, 2021.

[5] Catalin Cimpanu, **"BlackMatter Ransomware Says It's Shutting Down Due to Pressure from Local Authorities,"** *The Record,* November 3, 2021.

[6] Europol, **"12 Targeted for Involvement in Ransomware Attacks Against Critical Infrastructure,"** November 17, 2021.

[7] Carly Page, **"US Charges Kaseya Hacker and Seizes $6M from REvil Ransomware Gang,"** *TechCrunch*, November 8, 2021.

[8] Sergiu Gatlan, **"US Sanctions Chatex Cryptoexchange Used by Ransomware Gangs,"** *BleepingComputer*, November 8, 2021.

[9] Danny Palmer, **"Ransomware: Suspected REvil Ransomware Affiliates Arrested,"** *ZDNet*, November 8, 2021.

[10] Michael Gariffo, **"US Cyber Command Head Confirms Direct Actions Against Ransomware Gangs,"** *ZDNet*, December 8, 2021.

[11] Catalin Cimpanu, **"FSB Arrests REvil Ransomware Gang Members,"** *The Record*, January 14, 2022.

[12] FBI, Cyber Division, **"Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ranswomware Attacks,"** September 1, 2021.

[13] Lawrence Abrams, **"US Farmer Cooperative Hit by $5.9M BlackMatter Ransomware Attack,"** *BleepingComputer*, September 20, 2021.

[14] HIPAA Journal, **"Scripps Health Ransomware Attack Cost Increases to Almost $113 Million,"** August 18, 2021.

[15] Cybersecurity and Infrastructure Security Agency, **"Alert (AA20-302A): Ransomware Activity Targeting the Healthcare and Public Health Sector,"** November 02, 2020.

[16] Joshua Shilko et al., **"FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets,"** Mandiant, October 7, 2021.

[17] Check Point, **"Ransomware Attacks Continue to Surge, Hitting a 93% Increase Year Over Year,"** June 14, 2021.

[18] Justin Couchot, **"Butte County Bus System Hit by Weekend Cyberattack,"** *Chicoer*, July 8, 2021.

[19] Catalin Cimpanu, **"Ransomware Attack Disrupts Toronto's Public Transportation System,"** *The Record*, November 1, 2021.

[20] Lawrence Abrams, **"Trucking Giant Forward Air Reports Ransomware Data Breach,"** *BleepingComputer*, September 29, 2021.

[21] Jackeline Brown and Megan Brown, **"TSA Rail Cybersecurity Directives Show Increasing Government Regulation of Critical Infrastructure and the Private Sector,"** JDSupra, December 6, 2021.

[22] Kareem Fahim, **"Officials Say Cyberattack Crippled Gas Stations Across Iran,"** *The Washington Post*, October 26, 2021.

[23] Santosh Janardhan, **"More Details About the October 4 Outage,"** Engineering at Meta, October 5, 2021.

[24] Sam Curry, **"REvil Ransomware Attacks: Implications for Kaseya, MSPs and Businesses,"** Cybereason, July 7, 2021.

[25] Catalin Cimpanu, **"Microsoft Says Russia Hacked At Least 14 IT Service Providers This Year,"** *The Record*, October 25, 2021.

[26] MikroTik, **"Mēris Botnet,"** September 15, 2021.

[27] Vivek Ganti and Omer Yaochimik, **"A Brief History of the Meris Botnet,"** Cloudflare, November 9, 2021.

[28] Qrator, **"Mēris Botnet, Climbing the Record,"** September 9, 2021.

[29] Go Programming Language, **"Go."**

[30] Ofer Caspi, **"AT&T Alien Labs Finds New Golang Malware (BotenaGo) Targeting Millions of Routers and IoT Devices with More than 30 Exploits,"** AT&T Cybersecurity, November 11, 2021.

[31] Ravie Lackshmanan, **"Notorious Emotet Botnet Makes a Comeback With the Help of TrickBot Malware,"** *The Hacker News*, November 16, 2021.

[32] FEODO Tracker, **"Browse Botnet C&Cs,"** accessed November 22, 2021.

[33] Victoria Kivilevich, **"All Access Pass: Five Trends with Initial Access Brokers,"** KELA, August 2, 2021.

[34] Catalin Cimpanu, **"CISA Creates Catalog of Known Exploited Vulnerabilities, Orders Agencies to Patch,"** *The Record*, November 3, 2021.

[35] National Security Agency and Cybersecurity and Infrastructure Security Agency, **"Selecting and Hardening Remote Access VPN Solutions,"** September 2021.

[36] GitHub, **"Embedded Malware in coa,"** November 4, 2021.

[37] Catalin Cimpanu, **"Malware Found in npm Package with Millions of Weekly Downloads,"** *The Record*, October 23, 2021.

[38] Ravie Lackshmanan, **"Malicious NPM Libraries Caught Installing Password Stealer and Ransomware,"** *The Hacker News*, October 28, 2021.

[39] Catalin Cimpanu, **"Python Packages Caught Attemping to Steal Discord Tokens, Credit Card Numbers,"** *The Record*, July 29, 2021.

[40] Simon Scannell, **"Agent 007: Pre-Auth Takeover of Build Pipelines in GoCD,"** SonarSource, October 27, 2021.

[41] USCYBERCOM Cybersecurity Alert, @CNMF_CyberAlert, **"Mass Exploitation of Atlassian Confluence CVE-2021-26084,"** September 3, 2021.

[42] Mark Ellzey, **"CVE-2021-26084-Confluenza,"** Censys, September 2, 2021.

[43] Catalin Cimpanu, **"GitLab Servers are Being Exploited in DDoS Attacks in Excess of 1 Tbps,"** *The Record*, November 4, 2021.

[44] Jake Baines, **"GitLab Unauthenticated Remote Code Execution CVE-2021-22205 Exploited in the Wild,"** Rapid7, November 1, 2021.

[45] National Security Agency et al., **"Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments,"** July 2021.

[46] Nir Ohfeld and Sagi Tzadik, **"ChaosDB Explained: Azure's Cosmos DB Vulnerability Walkthrough,"** WIZ, November 10, 2021.

[47] Nir Ohfeld and Alon Schindel, **"'Secret' Agent Exposes Azure Customers to Unauthorized Code Execution,"** WIZ, September 14, 2021.

[48] Taylor Mullins and Mo Cashman, **"OMIGOD Vulnerability Opening the Door to Mirai Botnet,"** McAfee, September 22, 2021.

[49] Ariel Zelivansky and Yuval Avrahami, **"What You Need to Know About Azurescape,"** Palo Alto Networks, September 9, 2021.

[50] Microsoft Offensive Research & Security Engineering Team, **"A Deep-dive Into the SolarWinds Serv-U SSH Vulnerability,"** Microsoft, September 2, 2021.

[51] Randori Attack Team, **"Zero-Day Disclosure: Palo Alto Networks GlobalProtect VPN CVE-2021-3064,"** Randori, November 10, 2021.

NOZOMI NETWORKS

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

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

NN-SEC-RP-FULL-2021-2H-001

nozominetworks.com