



RESEARCH REPORT

OT/IoT Security Report

**What You Need to Know to Fight
Ransomware and IoT Vulnerabilities**

July 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](https://nozominetworks.com/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

4



2. Ransomware Insights

9

2.1 Introduction

10

2.2 Notable Ransomware Attacks

13

2.3 Recommendations

16



3. Vulnerability Analysis

18

3.1 Introduction

19

3.2 Recommendations

23



4. IoT Security Camera Spotlight

24

4.1 Introduction

25

4.2 Recommendations

32



5. Conclusions

34

5.1 What You Need to Know to Fight Ransomware and IoT Vulnerabilities

35



6. References

37

1. Executive Summary

The first half of 2021 signaled a new dawn for the COVID-19 pandemic, with proof that immunization programs can dramatically reduce infection rates and disease severity.¹ With a return to normal in sight for some countries with advanced economies, the global economy expanded at a rate of 5.6 percent—the strongest post-recession pace in 80 years.²

At the same time, cybercrime has continued to rise sharply, perhaps fueled by its potential for profit, while on the other hand, workforces are overwhelmed and vulnerable. Ransomware attacks, for example, are estimated to have grown 116% between January and May of this year³ and ransomware payments are increasing.⁴

To help defenders of OT/IoT environments and the security community, this report focuses on three important areas: ransomware, new vulnerability disclosures and the security risks of IoT security cameras. It provides insights for re-evaluating your risk models and security programs, along with actionable recommendations for securing operational systems.

Ransomware

Ransomware dominated the news headlines in the first half of 2021, particularly with the attack on Colonial Pipeline. While this notable incident did not include a direct breach of the OT network, pipeline systems were taken offline by the company, resulting in gas shortages along the U.S. East Coast.

This highlights the linkage between IT and OT risks. Even if the attack did not cross from IT to OT, operational systems were disrupted out of an abundance of caution with regards to safety.

Ransomware threats are now a board-level topic of conversation. All organizations with OT systems need to understand how these attacks are conducted and how to defend against them.

Modern ransomware attacks are increasingly executed by criminal groups using the Ransomware as a Service (RaaS) model. These groups run much like a cartel, motivated by profit and involving multiple unrelated parties acting together in an ecosystem.



MOST NOTABLE ATTACK - FIRST HALF OF 2021

Colonial Pipeline Ransomware Attack

RANSOM PAID

\$4.4 million

OT IMPACTS

While the OT network was not directly breached, pipeline systems were taken offline. The company had significant losses stemming from six days of downtime and the costs of recovery.

Darkside, the group that attacked Colonial Pipeline, is an example of a RaaS. It coordinates an effort that carefully prepares and deploys malware that uses a combination of attack techniques. Often, this leads to the successful extortion of its victims.

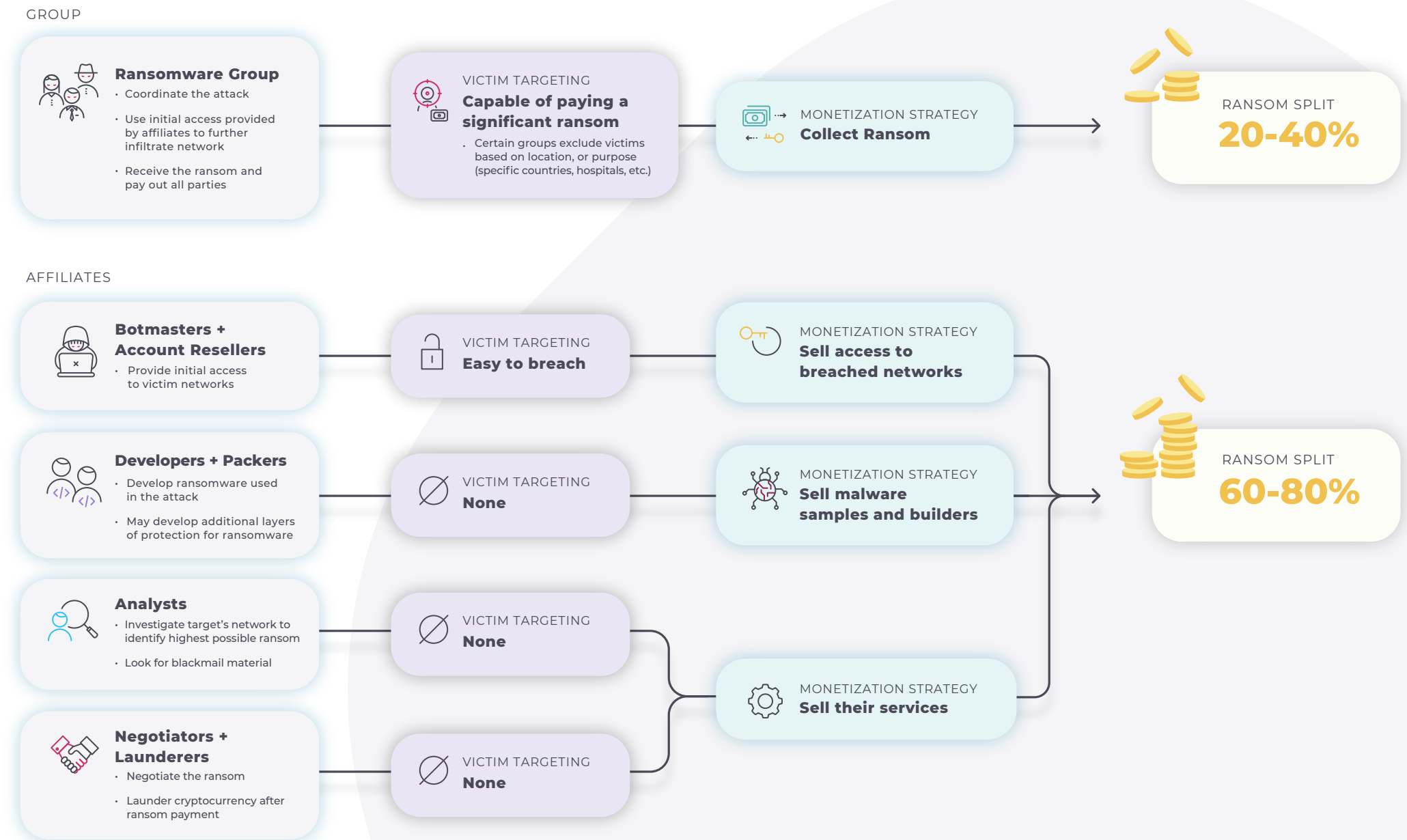
Nozomi Networks Labs studied the internals of the DarkSide executable and revealed the malware’s techniques in three areas:

- Selecting victims and files
- Ensuring anonymity and anti-detection
- Preventing data restoration

The success of the entire attack shows the effectiveness of the RaaS model, with a division of labor that plays to the strengths of each party.

Unfortunately, another RaaS operator, REvil, also flourished in the first half of the year with high profile attacks on JBS Foods, Acer, and Quanta, amongst others. This group is setting new records with ransom demands of \$50 million or more, and having tremendous impacts on business—further emphasizing the high risk organizations face from this type of threat.

Sample Ransomware as a Service Ecosystem



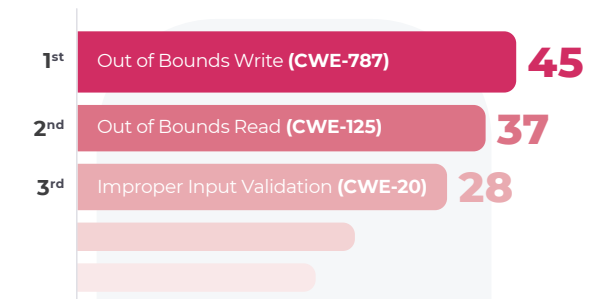
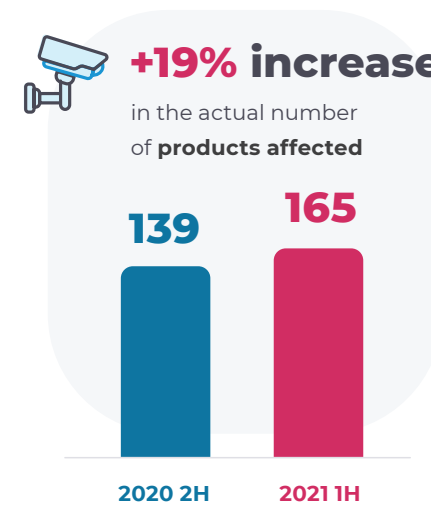
Vulnerability Research

Vulnerabilities published by ICS-CERT⁵ increased 44% in the first half of 2021 as compared to the second half of 2020. While the number of vendors affected rose by just 5%, the number of products rose 19%.



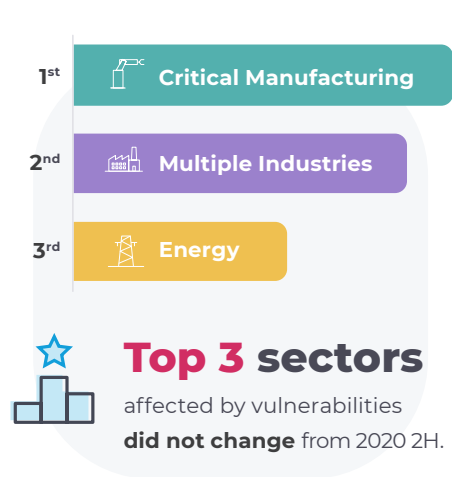
The top three industries affected include Critical Manufacturing, a grouping identified as Multiple Industries, and Energy. The key industry trend is that vulnerabilities solely affecting the Critical Manufacturing sector rose by 148%. This poses an additional challenge to an industry where many segments are struggling to regain momentum from pandemic-driven shutdowns.⁶

ICS Vulnerability Trends

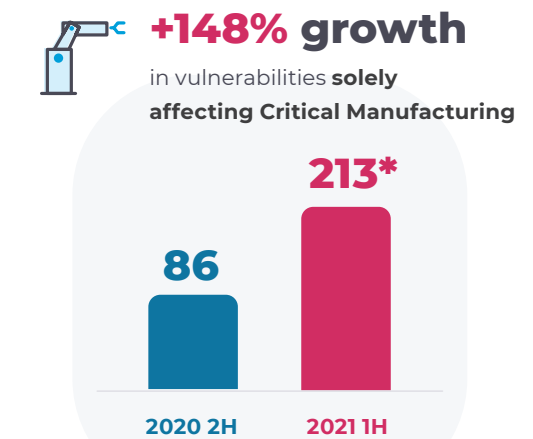
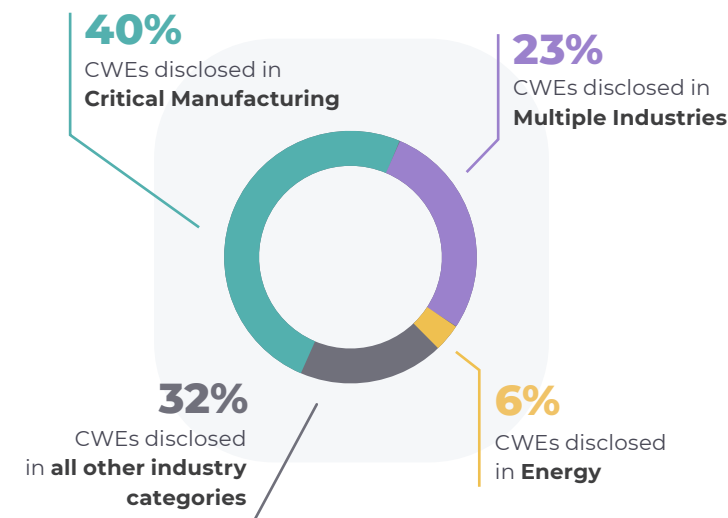


Most-disclosed CWEs

Compared to 2020 2H, CWE-787 had a +64% increase, while CWE-125 and CWE-20 each dropped down one place.



Top 3 sectors affected by vulnerabilities **did not change** from 2020 2H.



When the 95 vulnerabilities from other industry groupings* are included, the total is 308 for 2021 1H.

* Other industry groupings refers to vulnerabilities that CISA indicates involve a group that includes, for example Commercial Facilities, Energy and Critical Manufacturing. CISA also has "Multiple" and "Multiple Sector" groups of vulnerabilities, which do not identify specific industries, and thus those numbers have not been included in industry-specific statistics.

IoT Security Camera Vulnerabilities

Today's OT networks are very different than the OT networks of ten years ago. The fourth industrial revolution and pandemic-fueled digital transformation are driving the convergence of IT and OT. OT environments now include more off-the-shelf-technology, including IT machines and IoT devices.

IoT security cameras are an example of a device that is used extensively by many organizations, including those in industrial sectors. The global video surveillance market size is expected to grow from US \$45.5 billion in 2020 to US \$74.6 billion by 2025, with use by

the infrastructure sector growing the fastest.⁷

Over the last six months, Nozomi Networks has discovered and disclosed three surveillance camera vulnerabilities for companies that use Peer-to-Peer (P2P) functionality to provide remote access to audio/video streams.

We examined cameras from both Reolink and ThroughTek in our lab. While Reolink develops and uses its own P2P functionality, ThroughTek provides a P2P SDK that is used by many original equipment manufacturers (OEMs) of security cameras and IoT devices.

Our research revealed vulnerabilities for both vendors that allow anyone who gains access

to users' audio/visual (A/V) streams to see the data in cleartext.

Furthermore, in certain scenarios, the P2P vendor has access to cleartext A/V streams and can access local user lists and passwords. This is a striking violation of confidentiality expectations.

In March of this year, a very public security camera cyberattack occurred. The affected vendor was Verkada and the outcome was that perpetrators gained access to the live video feeds of thousands of surveillance cameras.

The entry point for the attack was an internet-exposed support server. From there, the threat actors obtained privileged account credentials that eventually allowed access to A/V streams.

While remote viewing of A/V streams is a popular capability, careful due diligence is required when selecting a product and a vendor. It's important to know what technology is used to provide remote access and what measures the vendor has taken to ensure cybersecurity and data privacy.



The Live Video Feeds of 150,000 Security Cameras were Exposed in the Verkada Cyberattack

Attackers were also able to execute shell commands on breached cameras, providing an entry point for lateral movement on victims' networks. **This could lead to consequences such as data theft, ransomware deployment or system disruption.**

VIDEO SURVEILLANCE MARKET SIZE GROWTH EXPECTATION



From
in 2020

US \$45.5 billion >

to

US \$74.6 billion
by 2025

Conclusions and Recommendations

A successful ransomware attack can be extremely debilitating, leaving victims with no other option than to meet the hackers' demands. Taking proactive steps to prevent ransomware infection is key to significantly reducing risk.

The first area to focus on for ransomware prevention is reducing opportunities for initial access to your networks. This includes having spear-phishing protection in place, implementing security awareness training, and requiring multi-factor authentication wherever possible.

Strengthening defense in depth measures, as per the cybersecurity standard most relevant to your organization, is also important.

With ransomware attacks increasing in frequency and sophistication, adopt a post-breach mindset. For example, have a detailed plan for a failure in IT that could impact OT, complete with operational continuity and disaster recovery components.

With regards to vulnerabilities, simply knowing the numbers for a given timeframe is not the way to assess risk. Instead, assess your security fundamentals against major threats, like REvil or emerging new ransomware, and harden your attack surface.

When selecting an IoT device, bear in mind that these devices are often insecure-by-design. If you need a capability like remote viewing of surveillance video, do your due

diligence on the technology and vendors under consideration.

As the pandemic becomes more manageable and economies strengthen, cybercrime will continue to rise.

To help network defenders, this report includes ten actionable measures to take now to protect your operations.

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 with 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 and confidentiality of your operational systems.

TEN MEASURES TO TAKE IMMEDIATELY



Malware Infection Prevention



OT Network Monitoring



Network Segmentation



Threat Intelligence



Secure Remote Access



Post-Breach Mindset



Disaster Recovery Planning



Attack Surface Reduction



IoT Vendor and Device Selection

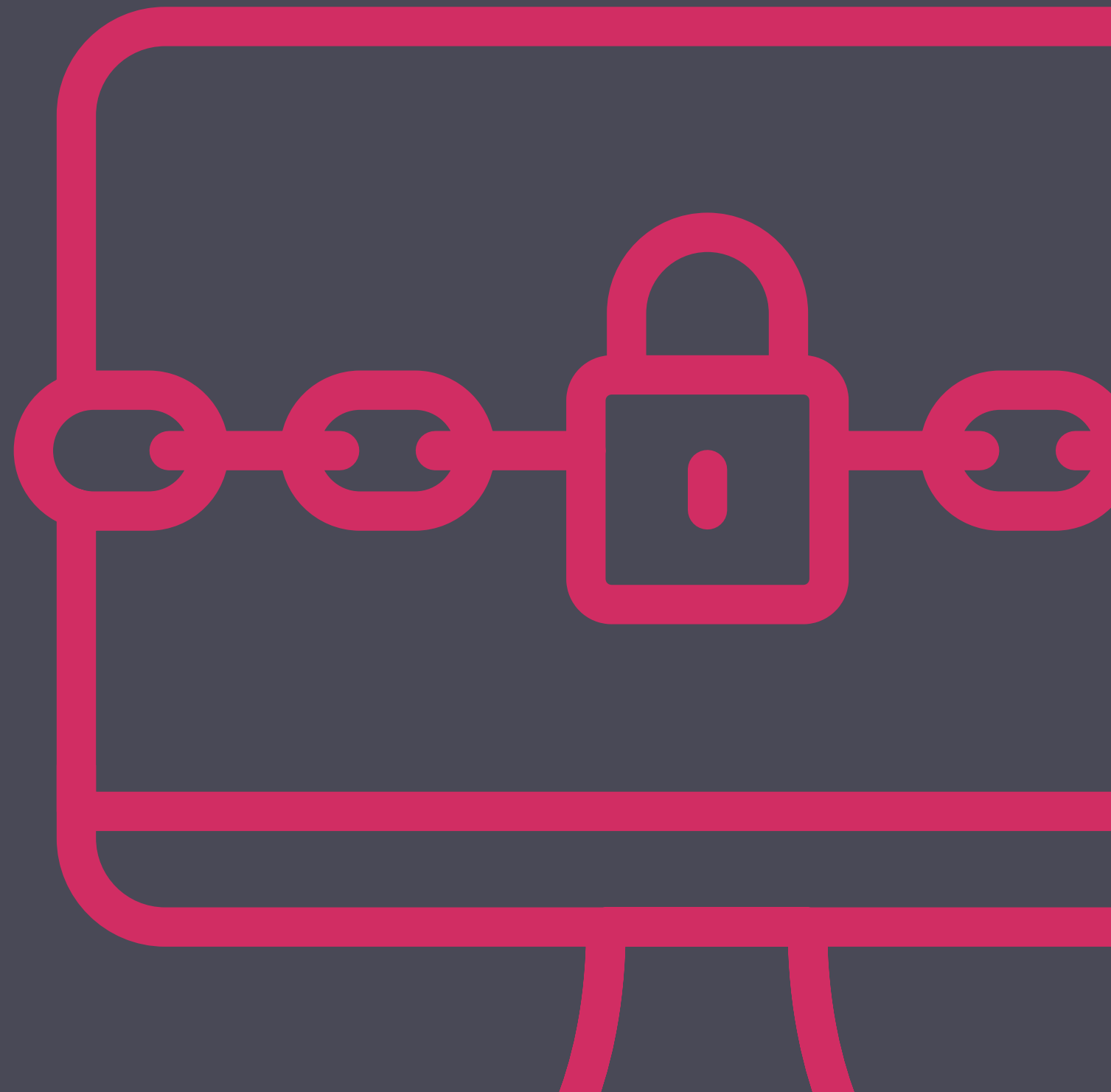


IoT Network Monitoring

2

Ransomware Insights

2.1 Introduction	10	2.3 Recommendations	16
2.1.1 Ransomware as a Service (RaaS)	10	2.3.1 Malware Infection Prevention	16
2.1.2 The RaaS Ecosystem	11	2.3.2 OT Network Monitoring	16
2.1.3 Ryuk and the Ransomware Kill Chain	12	2.3.3 Network Segmentation	16
2.1.4 Automated Attack Execution	12	2.3.4 Threat Intelligence	16
2.2 Notable Ransomware Attacks	13	2.3.5 Secure Remote Access	16
2.2.1 DarkSide Attack on Colonial Pipeline	13	2.3.6 Adopting a Post-Breach Mindset	17
2.2.2 REvil Attack on JBS Foods and Others	14	2.3.7 Disaster Recovery Planning	17
2.2.3 Timeline of Notable Year-to-Date Ransomware Attacks	15		





2.1 Introduction

Ransomware attacks have been increasing in frequency and impact over the past several years, with attacks on industrial organizations rising 500% between 2018 and 2020.⁸ The high rate of growth continues upwards this year, with another 116% increase just between January and May of 2021.⁹

Such attacks reached new heights in May with the ransomware attack on Colonial Pipeline, a company that transports 45% of the U.S. East Coast fuel supply.¹⁰ The attack affected some of the company's IT systems and in response, the company took certain systems offline to contain the threat, temporarily halting all pipeline operations.¹¹ While the OT network was not directly breached, the outcome was a six-day period of gas shortages.

Next, a ransomware attack hit JBS Foods, a major meat processing company with facilities across the U.S., Australia, the UK, and other countries.¹² This threat to our food supply also hit the headlines, significantly raising ransomware awareness for the public, governments, and critical infrastructure asset owners.

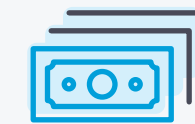
While neither of these attacks was executed against operational systems, each resulted in disruptions to those systems. The outages, and the media attention they generated, elevated cybersecurity discussions in board rooms around the world. It's critical that all organizations with OT systems understand how modern ransomware attacks are conducted and how to defend against them.

2.1.1 Ransomware as a Service (RaaS)

Many of today's ransomware attacks involve shadowy organizations that communicate on darknet forums—but they are anything but lightweight in terms of how they conduct their operations.

While some ransomware groups are large enough to work independently and carry out every step of an attack themselves, this approach is waning. Increasingly, the Ransomware as a Service (RaaS) model, which involves many players, is gaining popularity.

The coordinated action of different parties working together, each playing to their strengths, makes ransomware groups powerful adversaries. And, with multi-step, always evolving malware available for purchase, the criminals driving ransomware attacks do not need technical skills themselves.



Ransomware Losses Are Escalating

RANSOM PAYMENTS

+43%

between Q4 2020 and Q1 2021, jumping from \$154,108 to \$220,298.¹³

TOTAL LOSSES EXPECTED TO REACH

\$20 billion

this year from global ransomware damage.¹⁴



2.1.2 The RaaS Ecosystem

DarkSide, the group made famous by its attack on Colonial Pipeline, is one example of a modern RaaS group.

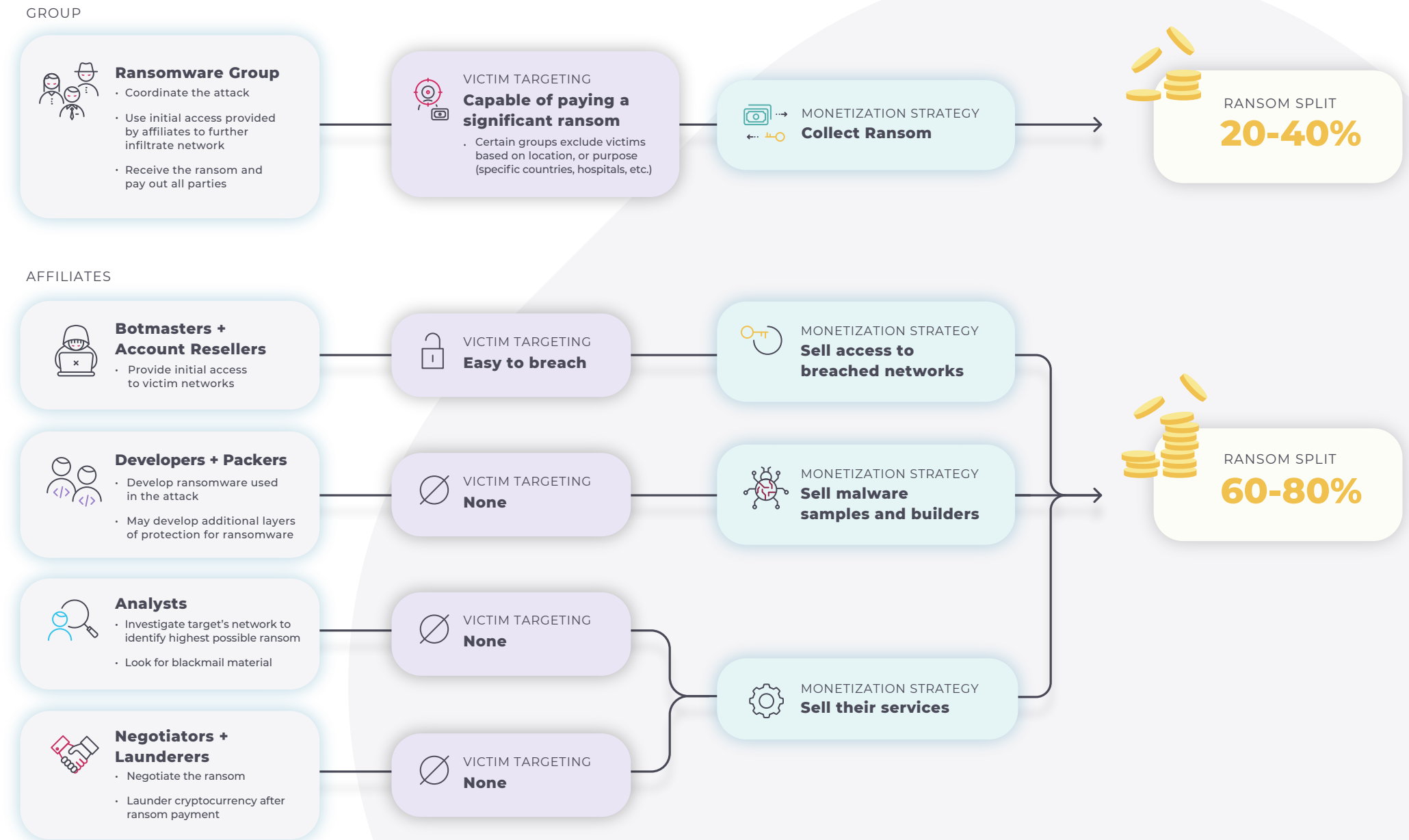
These groups run much like a cartel, motivated by profit and involving multiple, unrelated parties acting together in an ecosystem.

For example, experienced malware writers focus on the development of the core ransomware code, while other parties specialize in gaining access to networks or negotiating ransoms.

The diagram to the right shows one model of the players involved in a RaaS organization.

The structure is fluid, however, with different ransomware groups using various combinations of roles and ransom splits.¹⁵

Sample Ransomware as a Service Ecosystem





2.1.3 Ryuk and the Ransomware Kill Chain

In addition to the multiplicity of players involved in executing a ransomware attack, the malware itself is often made of multiple components.

A prime example is the kill chain used by **Ryuk** ransomware group. The diagram below shows eight different components, each of which might be sourced from different developers.

Ryuk also stands out for the speed of its attacks. Depending on the targeted

network, the length of time from infection to ransomware execution can be as little as a couple of hours.

This group is particularly heinous because of its targeting of healthcare facilities, which are already under pressure dealing with the COVID-19 pandemic.

Ryuk is estimated to have collected **over \$150 million in ransom**, with an average ransom of \$750,000 from each victim. Their largest confirmed payment came to 2,200 bitcoin, or approximately \$34 million.¹⁶

2.1.4 Automated Attack Execution

Once a ransomware attack starts, it proceeds automatically. No further commands are needed to complete the compromise.¹⁷

For network defenders, the challenge of understanding what's happening on the network during a ransomware attack, and reacting quickly enough, is significant.

The best defense is to prevent the attack in the first place, and tips on this are provided in the Recommendations section.



Paying Up Doesn't Always Pay Off

80%

of organizations who pay a ransom experience another attack. Nearly half of victims believe the second attack is by the same threat actors.¹⁸

8%

of ransomware victims fully recover their data. On average, those that paid only got back 65% of encrypted files, and 29% could only restore less than half.¹⁹

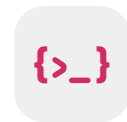
Ryuk Kill Chain



Phishing email



BazarLoader execution



Cobalt Strike deployment



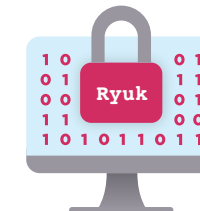
Domain discovery



ZeroLogon against DC



Additional asset discovery



Ransomware deployment



2.2 Notable Ransomware Attacks

2.2.1 DarkSide Attack on Colonial Pipeline

The malware DarkSide deployed against Colonial Pipeline is a good example of similar malware attacking organizations around the globe. Carefully prepared and deployed, it uses a combination of techniques to successfully extort its victims.

Nozomi Networks Labs studied the internals of the DarkSide executable, and revealed the techniques used by its machine code in three areas: selecting victims and files, ensuring anonymity and anti-detection, and preventing data restoration. The full details of our findings,

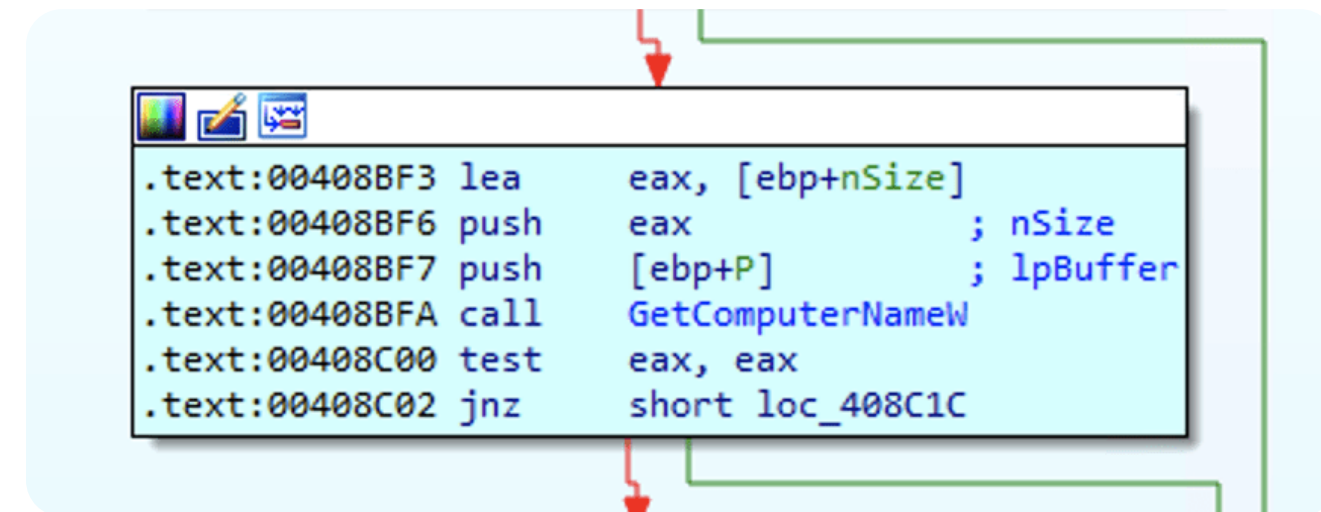


complete with screenshots and code samples, are described in the related blog.²⁰ Following is a summary of what we found.

Selection of Victims and Files

The malware first collects basic information about its victim's computer systems to learn the details of the technical environment. It skips victims from certain geographical regions by checking the language used by their systems. (Notably, DarkSide does not attack systems that use Russian or other Eastern European languages.²¹)

Next, DarkSide determines what files to encrypt. If malware attempts to encrypt all the files available on the system, it quickly makes the system unusable—leaving the victim without information on how to contact the attackers. The time required to encrypt all the files also slows the attack. For both these reasons, DarkSide is particularly selective about the files it encrypts, examining file directories, names and extensions.



The malware obtains the affected computer's name.

Preventing Data Restoration

If system administrators could quickly and easily restore the affected data without paying money to criminals, ransomware attacks would not succeed. The authors of DarkSide incorporate multiple techniques to ensure ransom is paid:

- **Backup Destruction:** DarkSide ensures that standard backup solutions are

unusable on targeted machines. It also attempts to disable various backup solutions by searching for them by name and deleting them.

- **Symmetric and Asymmetric Encryption:** To balance the need to encrypt with the need to encrypt quickly, DarkSide encrypts victims' files with a symmetric encryption algorithm and then encrypts the symmetric keys with their asymmetric public key.



DarkSide is just one example of a modern ransomware family that combines multiple time-tested techniques to achieve its goal. It also highlights the effectiveness of the RaaS model—with a division of effort that plays to the strengths of each party, threat actors have found a lucrative strategy to optimize their capabilities.

In the case of DarkSide, it is estimated that their more than 40 victims have paid \$90 million in total bitcoin, with \$15.5 million going to the development group and \$74.7 million going to affiliates.²²



Victims
40+



Amount Paid (in bitcoin)
\$90 million

Note that our blog on this topic includes DarkSide IOCs and a script for decrypting embedded strings.

Some final words on DarkSide—on May 13, 2021, the group announced it was shutting down

its operations, providing decryptors to all their affiliates for the targets they attacked, and paying all outstanding financial obligations. It is speculated that media and government attention led them to retreat underground.²³ The U.S. Department of Justice, for example, recovered \$2.3 million of the \$4.4 million ransom paid by Colonial Pipeline.²⁴

DarkSide's actions were followed by other ransomware operators and forums shutting down public operations. It is speculated these groups will likely resurface in the future, with different names and updated ransomware code.

2.2.2 REvil Attack on JBS Foods and Others

REvil, also known as Sodinokibi, is a RaaS operator that was particularly active in the first half of 2021.

In March, the computer manufacturer Acer's office network was hit—none of

the company's production systems were disrupted. The hackers demanded \$50 million for a decryptor, vulnerability report and deletion of stolen files. Acer countered with an offer of \$10 million, but it's unknown if any payment was made.^{25, 26}

REvil followed up the Acer attack with one on Quanta, which manufactures MacBooks for Apple. The cyber criminals claimed to have stolen blueprints for Apple's latest products and demanded a \$50 million ransom. Apparently Quanta did not pay the ransom and REvil went after Apple instead.²⁷

In May, REvil conducted its infamous attack on JBS Foods, the largest meat producer in the world, forcing it to shut down all its U.S. beef plants. It also disrupted other American, Canadian and Australian facilities, affecting the global supply chain. The company paid an \$11 million ransom to help restore operations.²⁸

At the time of publishing this report, REvil continues to make waves with its attack on Kaseya, a provider of a Software as a Service network management tool. This cunning supply chain/ransomware attack

is estimated to have impacted up to 1,500 organizations in dozens of countries around the world, including a supermarket chain in Sweden, schools in New Zealand and hundreds of U.S. companies. REvil has demanded a \$70 million ransom.²⁹



Such an attack can be particularly insidious to address. Once a breach happens, the victim would generally reach for these tools to work their way out of a bad situation, but when the tool itself is the problem, or is unavailable, it adds complexity to the recovery efforts.

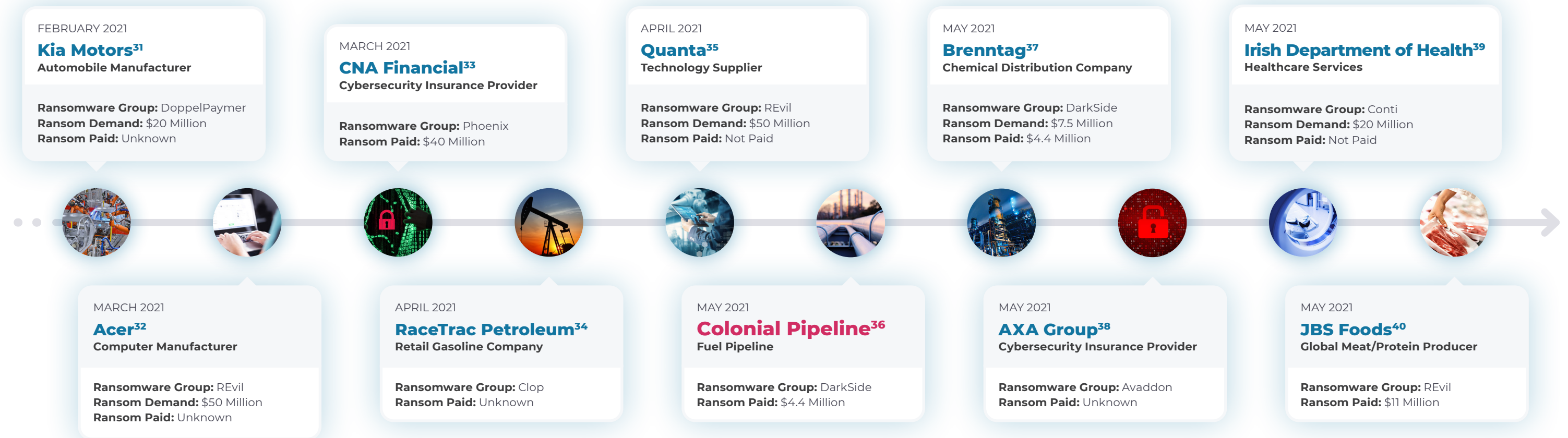
Chris Grove, Technology Evangelist, Nozomi Networks in response to the Kaseya attack³⁰

Like Darkside, the REvil ransomware group is believed to be based in Russia. Unlike Darkside, its notoriety has not yet forced it to shut down operations.



2.2.3 Timeline of Notable Year-to-Date Ransomware Attacks

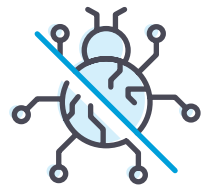
The events shown here are examples of ransomware attacks from around the world that either disrupted operations or involved large ransom demands.





2.3 Recommendations

2.3.1 Malware Infection Prevention



A successful ransomware attack can be extremely debilitating, leaving victims with no other option than to meet the

hackers' demands. At the same time, there are proactive steps your organization can take to significantly reduce risk.

Following security best practices and educating employees on security hygiene will reduce the likelihood of a breach. The first area to focus on is reducing the opportunity for initial access to your networks. This includes:

- Mail content scanning and filtering to thwart malicious campaigns
- Security awareness among all employees to avoid falling victim to phishing campaigns

2.3.2 OT Network Monitoring



Since the initial access is often gained separately from and prior to the actual ransomware attack, it's important to continually

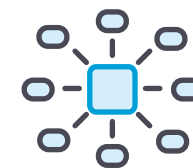
monitor networks for intrusions and mitigate vulnerabilities as quickly as possible.

Even if a group has access to your networks, it may be possible to stop the threat before that access is used for an attack. Ransomware groups often remain inside target networks for extended periods of time, moving laterally to maximize their impact.

With OT network monitoring, 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 by taking further actions to stop malicious behavior.

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.

2.3.3 Network Segmentation



Prioritize robust segmentation between IT and OT networks with firewall rules that consider the requirements of each zone.

Within the OT environment, segment the network as per the best practices outlined in the IEC 62443 standard to restrict the lateral movement of ransomware.

2.3.4 Threat Intelligence



Traditional threat detection capabilities provide context around suspicious actors related to known threats.

For example, up-to-date threat intelligence with IoCs for BazaarLoader, which can signal the coming of Ryuk, helps identify intrusion and provide time for defensive action.

2.3.5 Secure Remote Access



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 carefully monitored 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 and network segmentation. 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 Microsoft⁴¹ and Google,⁴² detailing their experiences, are available.

2.3.6 Adopting a Post-Breach Mindset



In addition to changing your approach to cybersecurity, like implementing a Zero Trust model, adopting a post-breach mindset can

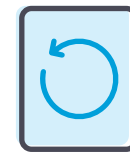
accelerate a cybersecurity cultural shift that increases resilience.

When an organization experiences a severe cybersecurity breach, they prioritize the cybersecurity conversation, mobilize budgets, and implement business continuity processes in a short amount of time. A post-breach mindset drives a dramatically lower likelihood of falling victim to a cyberattack.⁴³ What if you could gain all these benefits without experiencing the trauma and losses of a breach?

With ransomware attacks on industrial organization rapidly rising, it's safer to assume that you will be attacked rather than wonder if you will. And, planning for failures in IT that can impact OT helps everyone understand what it takes to maintain

operations safely. It's best to practice a mindset that asks: "We've been breached ... now what?"

2.3.7 Disaster Recovery Planning



A post-breach mindset should include a disaster recovery plan to handle scenarios where multiple

computer-based systems are affected simultaneously and production is dropped or halted completely. And, global organizations should thoroughly consider how they would handle disruptions impacting multiple geographies at the same time.

A characteristic case study would be Norsk Hydro, which suffered a ransomware attack in 2019, and forced to halt around 170 plants. Its response wasn't just action-oriented in terms of how quickly it responded to the technical challenges of the attack, but also on the communications side. The company choose to be completely transparent about the situation and was widely praised by the security community.⁴⁴

“Enterprises must now be prepared for the inevitable ransomware attack. That's why in addition to strengthening defenses, it's equally important to invest in business resilience in the face of an attack.

This post-breach mindset establishes a strong cybersecurity culture that asks the tough questions, anticipates worst-case scenarios and establishes a recovery and containment strategy aimed at maximizing your organization's resiliency, long before an attack occurs.

Edgard Capedevielle, CEO, Nozomi Networks, in response to the JBS Foods attack⁴⁵

3

Vulnerability Analysis

3.1 Introduction	19
3.1.1 ICS Vulnerabilities	19
3.1.1.1 Supply Chain Vulnerabilities	21
3.1.2 Medical Device Vulnerabilities	22
3.2 Recommendations	23
3.2.1 Attack Surface Reduction	23



3.1 Introduction

Industrial Control Systems (ICS) typically include many devices, both legacy and new, that are not designed with today's security requirements in mind. Over the last decade, industrial and OT networks have increasingly become targets, as researchers reveal more and more vulnerabilities that could be exploited by opportunistic threat actors.

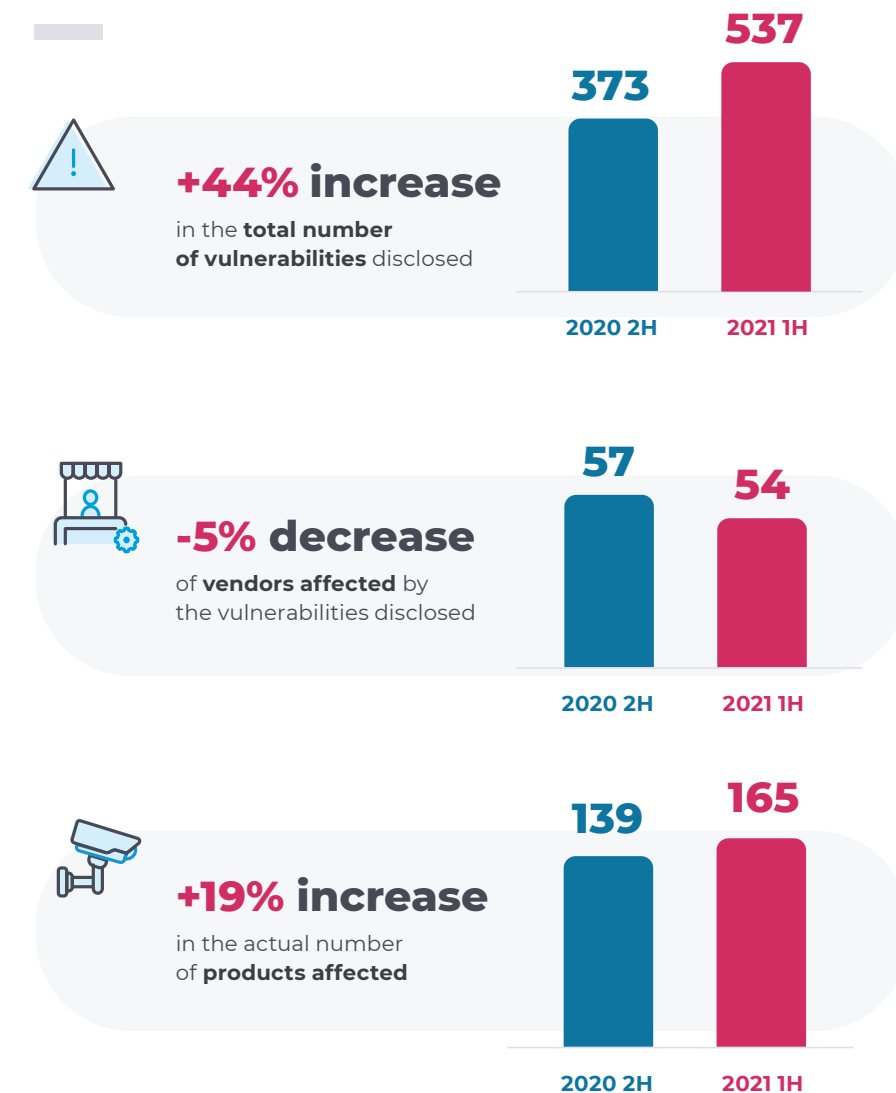
To help defenders, Nozomi Networks Labs analyzed the new vulnerabilities published by ICS-CERT, a program run by CISA, a U.S. government body.⁴⁶ While there are other sources of vulnerabilities than ICS-CERT, if a vulnerability is important, it is covered by ICS-CERT.

Vulnerabilities increased 44% in the first half of 2021 as compared to the second half of 2020. While the number of vendors affected rose by just 5%, the number of products rose 19%.

The top three industries affected include Critical Manufacturing, a grouping identified as Multiple Industries by CISA, and Energy. The most important detail of the industry breakdown is that vulnerabilities solely affecting the Critical Manufacturing sector rose by 148%. This poses an additional challenge to an industry where many segments are struggling to regain momentum from pandemic-driven shutdowns.⁴⁷

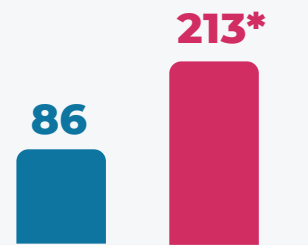
Analyzing new vulnerabilities helps organizations understand which ICS devices or software have recently come under public scrutiny and is an input into determining security priorities.

3.1.1 ICS Vulnerabilities





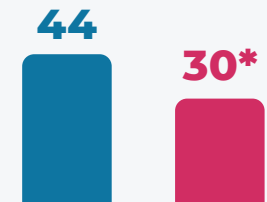
+148% growth
in vulnerabilities **solely**
affecting **Critical Manufacturing**



2020 2H 2021 1H

When the 95 vulnerabilities from other industry groupings* are included, the total is 308 for 2021 1H.

-32% decrease
in vulnerabilities **solely**
affecting the **Energy sector**

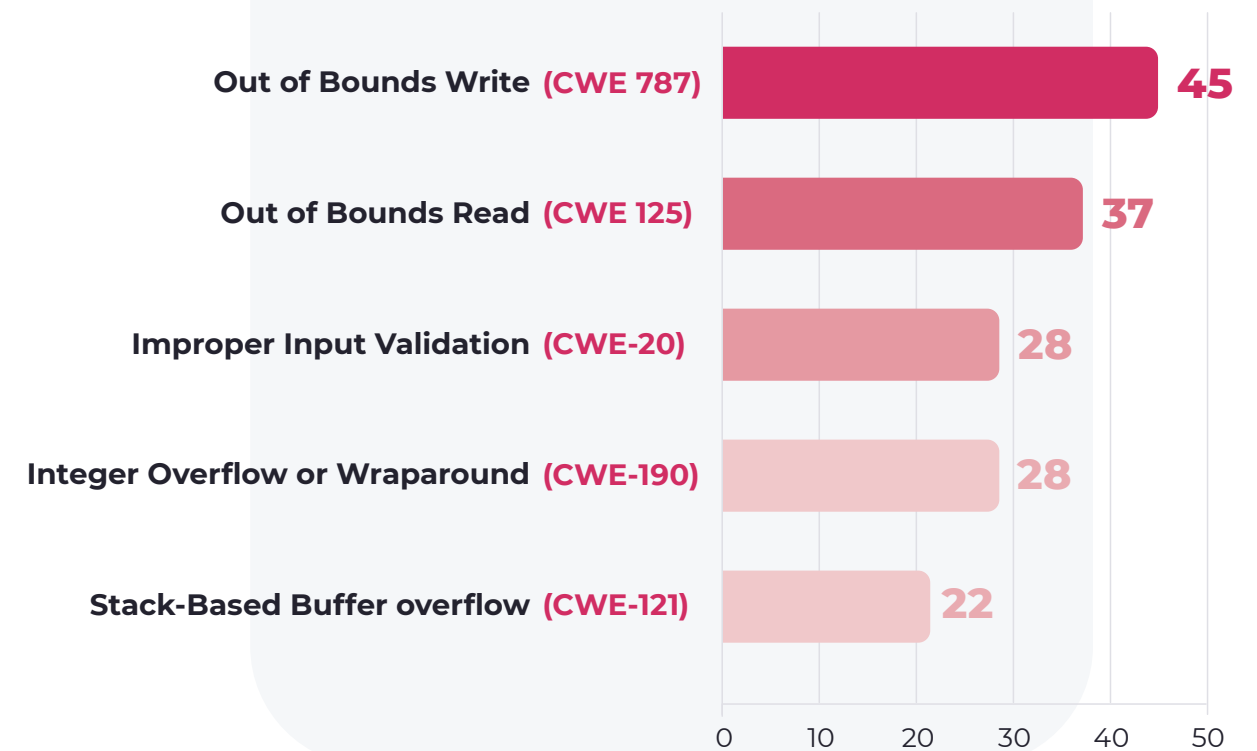


2020 2H 2021 1H

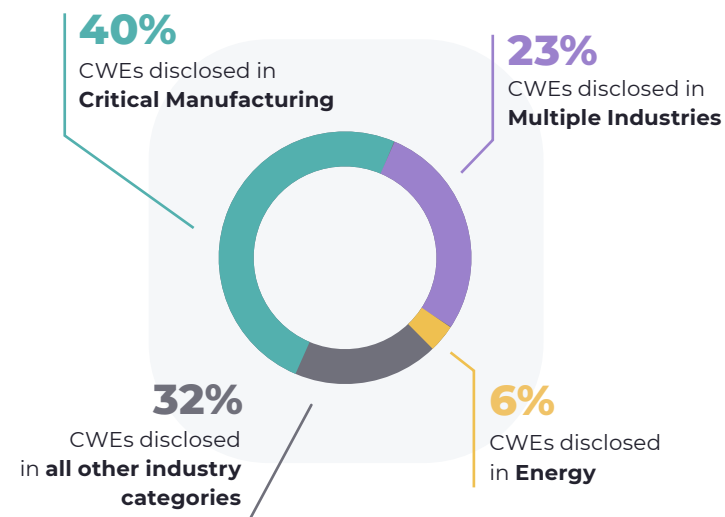
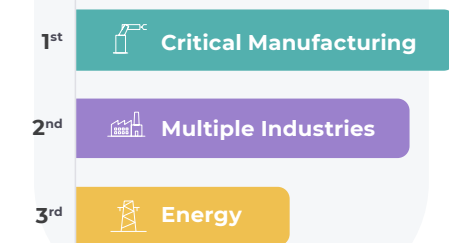
When the 133 vulnerabilities from other industry groupings* are included, the total is 163 for 2021 1H.

Most-disclosed CWEs in 2021

Compared to 2020 2H, CWE-787 had a +64% increase, while CWE-125 and CWE-20 each dropped down one place.



Top 3 sectors
affected by vulnerabilities
did not change from 2020 2H.



* Other industry groupings refers to vulnerabilities that CISA indicates involve a group that includes, for example Commercial Facilities, Energy and Critical Manufacturing. CISA also has "Multiple" and "Multiple Sector" groups of vulnerabilities, which do not identify specific industries, and thus those numbers have not been included in industry-specific statistics.



3.1.1.1 Supply Chain Vulnerabilities

Analyzing the raw data extracted from ICS advisories tells one aspect of the vulnerability story. A second aspect emerges when we perform a further, more specific analysis. Quite a few of the vulnerabilities disclosed in 2021 H1 are in fact related to the software supply chain behind ICS products. Software supply chain is a very broad term that doesn't necessarily capture the nuances of each specific situation.

For example, there are advisories such as [icsa-21-131-04](#),⁴⁸ where some of the documented vulnerabilities refer to known security issues in the secure remote access component from the vendor VNC.

SIEMENS
Ingenuity for life

The new advisory reflects the fact that it is now known that the Siemens product containing the VNC component has the vulnerabilities too. This advisory also shows how the vendor

itself—Siemens—is proactively researching and reporting issues to ICS-CERT.

Other advisories such as [icsa-21-019-01](#)⁴⁹ refer to new vulnerabilities in a software component, such as dnsmasq. In this case the software component is used in countless number of products, some of which are used in ICS.

Finally there are advisories such as [icsa-20-203-01](#),⁵⁰ initially released in 2020, that describe vulnerabilities in a license server used in ICS products. The advisory was recently updated to include new targets that are now known to be vulnerable.

For asset owners, the first step to improving security posture is to identify the products, and their components, that are reachable through the network.

This reveals the initial attack surface, and recommendations for securing it are provided in section 3.2.1.





3.1.2 Medical Device Vulnerabilities

Besides advisories for ICS, CISA also publishes vulnerability advisories for medical equipment. These advisories are labeled ICSMA to distinguish them. Although there are thousands of medical device manufacturers in the U.S., not to mention others made globally and used in the U.S., very few companies are coordinating vulnerability disclosures with CISA.⁵¹

In the first half of 2021 there were 537 ICS advisories disclosed and only 25 medical device ones.

The trend with ICS-CERT medical advisories is that each one bundles together several vulnerabilities.

Based on our experience researching vulnerabilities in this sector, this is an indication of two phenomena.

First, accessing medical devices and their corresponding software is a challenge

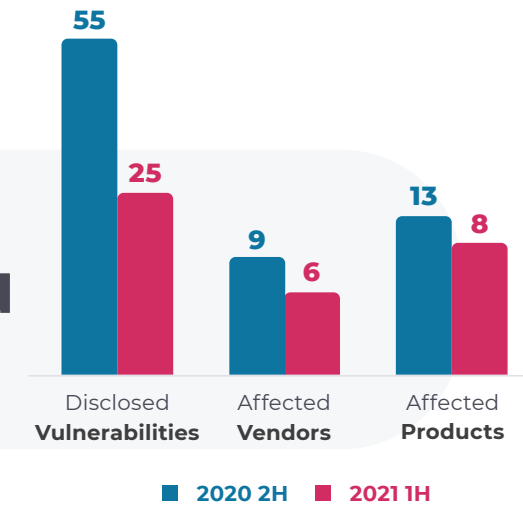
for security researchers. While this is understandable for scarce medical hardware during a pandemic, the software part of the equipment does not have the same intrinsic limitations. Nonetheless, the opportunity to conduct a security assessment of a medical software solution is a privilege for many researchers.

Second, based on data, it appears that medical platforms tend to have a high vulnerability density. This suggests that these products have a lower cybersecurity maturity level as compared to products that face the daily scrutiny of attackers, such as browsers.

The vulnerability data from the two periods shown in the charts to the right is too limited to assume that it represents a meaningful trend. It is simply a starting point for understanding the types of vulnerabilities in medical devices. Furthermore, the low number of vulnerabilities does not mean that these devices are inherently safer than other ICS devices—rather, it likely reflects limited research.



ICS medical advisories decreased in several areas



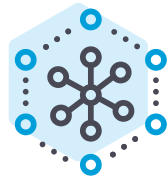
Medical Device Top CWEs Summary





3.2 Recommendations

3.2.1 Attack Surface Reduction



To reduce risk, organizations should carefully monitor their attack surface and limit the exposure of services to

those strictly required for proper operations.

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 the authentication and authorization of medical software programs.

CISA's recommendations for reducing exposure across operational technologies include a section on having a resilience plan, which applies equally to ICS and medical systems.⁵²



4

IoT Security Camera Spotlight

4.1 Introduction	25
4.1.1 Security Cameras and Remote Access to Audio/Visual Streams	25
4.1.2 P2P Architecture	26
4.1.3 Reolink Research Findings	27
4.1.4 ThroughTek Research Findings	29
4.1.5 Verkada Security Camera Breach	30
4.2 Recommendations	32
4.2.1 Vendor and Security Camera Selection	32
4.2.2 Deploy Network Monitoring Before Deploying IoT Devices	32



4.1 Introduction

IoT security cameras are used extensively by industrial and the critical infrastructure sectors. According to research firm Markets and Markets, the global video surveillance market size is expected to grow from US \$45.5 billion in 2020 to US \$74.6 billion by 2025.⁵³

The infrastructure sector—including transportation, city surveillance, public places, and utilities—is expected to have the highest growth rate during that period. Given the prevalence and growing use of IoT cameras, it's important to understand their security risks.

Over the last six months, Nozomi Networks has discovered and disclosed three surveillance camera vulnerabilities for companies that use Peer-to-Peer (P2P) functionality to provide access to audio/video streams. Additionally, we've reported on an IoT security camera cyberattack that resulted in unauthorized access to the live video feeds of 150,000 surveillance cameras and their full archive.⁵⁴

To protect organizations from security camera risk and contribute to the security community at large, we're sharing the insights we gained through researching surveillance system vulnerabilities. We also provide guidance on vendor considerations and how to mitigate risks.

4.1.1 Security Cameras and Remote Access to Audio/Visual Streams

Security cameras are often part of a system that provides remote access to audio/video (A/V) streams. This capability can be achieved with a P2P functionality, which involves sharing data over the internet.

The end user does not know exactly how the data is being transmitted or how secure the transmission is. Unfortunately, the data sharing technology being used is not necessarily secure.

The aim of P2P is to avoid having to explicitly configure a firewall to provide users with remote video data. Instead, a connection is established through a set technique commonly defined by the umbrella term "hole punching".

The technical details vary between vendors and third-party providers of this functionality. However, a typical scenario involves an internet-reachable node which acts as a mediator between the client who wants

to access the A/V stream and the device that serves the data. The device could be a camera or a network video recorder (NVR), a specialized device that stores video data.

In August 2020, security researcher Paul Marrapese published extensive research detailing security issues affecting the P2P implementations of some vendors.⁵⁵ By exploiting these vulnerabilities, an attacker can intercept the A/V stream at will.

What concerned Nozomi Networks Labs the most about Marrapese's brilliant work was the sheer number of end users affected by the problems identified, and the lack of official documentation describing how P2P functionality works.

By examining devices we had in our lab, it became clear that the privacy and security implications of using a camera's "P2P" feature are not clearly explained to users.



4.1.2 P2P Architecture

The P2P architecture used for remote video viewing is very similar across different vendors, including Reolink and ThroughTek. While Reolink develops and uses its own P2P functionality, ThroughTek provides a P2P SDK that is used by many OEMs of security cameras and IoT devices.

Here are the steps required for remote viewing of an A/V stream:

0. The Vendor P2P Server (V-P2P-S) is available as a host accessible on the internet.

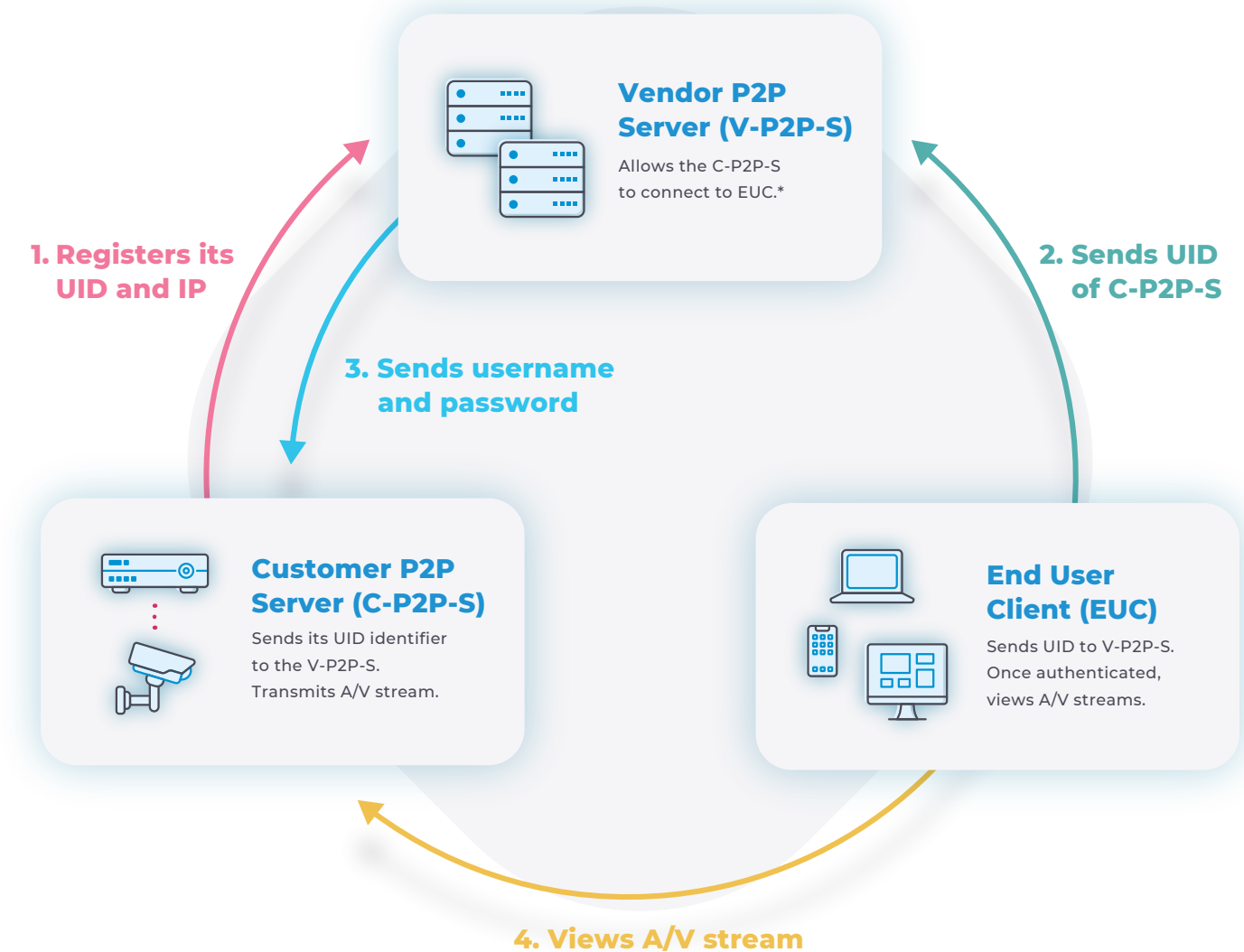
1. The Customer P2P Server (C-P2P-S) starts up and if the P2P functionality is active, communicates its UID and IP address to the V-P2P-S.

2. The End User Client (EUC) sends the V-P2P-S the UID of the C-P2P-S.

3. The V-P2P-S sends the EUC username/password to the C-P2P-S.

4. The EUC is authenticated and starts viewing the A/V stream.

Sample P2P Architecture Diagram



* In general, the V-P2P-S only handles the "directory" part of the protocol. It does not proxy the A/V stream. However, if the performance of the connection between the C-P2P-S and the EUC is low, it might proxy the A/V stream.



4.1.3 Reolink Research Findings

In our research lab we created a setup similar to the one described in the Reolink documentation and shown in the P2P architecture diagram on the previous page. Our scope, however, was limited to understanding how the A/V stream was secured when traversing the internet.

We used a combination of background research and reverse engineering to dissect and analyze the traffic between the

components of the P2P architecture. You can learn the technical details of how we did this in our blog on this topic.⁵⁶

Surprisingly, our findings showed that the communication between the NVR and the P2P client was lacking any sort of secure key exchange encryption. In our own tests we were able to reproduce the A/V content in cleartext.



Security Cameras with P2P Functionality Pose a **High Confidentiality Risk**

Anyone who gains access to client/NVR traffic can view the A/V stream. Furthermore, the P2P vendor also has access to cleartext A/V streams when the relay feature is used.



VULNERABILITIES DISCLOSED BY NOZOMI NETWORKS



Reolink P2P Protocol Deobfuscation and Credentials Leak — CVE-2020-25173

Vendor

Reolink

CWE-321

Use of Hard-coded Cryptographic Key

Equipment

P2P Protocol

CWE-319

Cleartext Transmission of Sensitive Information

Sector

Communications

Description

The communication between Reolink NVR, P2P servers and applications is obfuscated with a custom protocol that relies on a hardcoded key. By deobfuscating the protocol, it is possible to access the cleartext content of the communication. During the tests, this was observed to contain the P2P credentials.

Disclosure Date

Jan. 19, 2021

ICS Advisory

ICSA-21-019-02



In some situations, the connection between a client and the NVR is not stable enough. In these cases, the Reolink P2P implementation allows for the P2P server to act as a relay node, effectively behaving as a man-in-the-middle.

Coupling the lack of an end-to-end encryption with the relay feature de facto exposes the cleartext A/V stream to the vendor.

While investigating the protocol exchange between the Reolink P2P server and the NVR, we noticed another security issue. The vendor's server also pulls together the list

of local users registered with the NVR and their corresponding cleartext passwords.

The immediate consequence of this design is that an actor who can access this network traffic can fetch the local users' credentials. With a bit of protocol deobfuscation, they can log into the NVR using a regular Reolink client.

We struggle to understand why the vendor wants this sort of credential information and access.



P2P Security Camera Vendors Can View Video Streams and Access User Credentials

Vendors can view cleartext audio/visual streams and access local user lists and passwords—a striking violation of confidentiality expectations.



VULNERABILITIES DISCLOSED BY NOZOMI NETWORKS



Reolink P2P Video/Audio Lack of Encryption and Stream Reconstruction — CVE-2020-25169

Vendor

Reolink

Equipment

P2P Protocol

Sector

Communications

Disclosure Date

Jan. 19, 2021

ICS Advisory

ICSA-21-019-02

CWE-321

Use of Hard-coded Cryptographic Key

CWE-319

Cleartext Transmission of Sensitive Information

Description

Reolink P2P video/audio stream is transmitted without any encryption. Any actor who can access the client/NVR traffic as it traverses the internet can access its content with no confidentiality for the parties involved.



4.1.4 ThroughTek Research Findings

While the Reolink vulnerabilities applied to their own security cameras, the situation with ThroughTek is different.

ThroughTek creates a software component that is part of the supply chain for many original equipment manufacturers (OEMs) of consumer-grade security cameras and IoT devices. The company states that its solution is used by several million connected devices.⁵⁷

ThroughTek's P2P Software Development Kit (SDK) uses the same P2P design architecture as Reolink to provide remote access to audio/visual streams.

A peculiarity of P2P SDKs, though, is that OEMs are not just licensing a P2P software library. They also receive infrastructure services (the offsite P2P server) for authenticating clients and servers and handling the A/V stream.

We researched the ThroughTek P2P SDK by testing it with a NVR in our lab. The technical details of this work are detailed in our blog.⁵⁸



P2P Security Camera and IoT Vulnerabilities Are Widespread

ThroughTek's P2P SDK is used by many vendors, for millions of assets. It's difficult for organizations or individuals to know if this software component is used in their devices. The best way to ensure privacy and confidentiality is to disable remote viewing functionality.



VULNERABILITIES DISCLOSED BY NOZOMI NETWORKS



ThroughTek P2P SDK — CVE-2021-32934

Vendor

ThroughTek

Equipment

P2P SDK

Sector

Communications

Disclosure Date

June 15, 2021

ICS Advisory

ICSA-21-166-01

CWE-319

Cleartext Transmission of Sensitive Information

Description

The affected ThroughTek P2P products do not sufficiently protect data transferred between the local device and ThroughTek servers. This can allow an attacker to access sensitive information, such as camera feeds.



Our findings resulted in the discovery and disclosure of a vulnerability regarding the cleartext exposure of sensitive information.

The consequences of the vulnerabilities of both Reolink and ThroughTek are similar: since this traffic traverses the internet, an attacker who is able to access it can reconstruct the A/V stream.

Because ThroughTek's P2P library has been integrated by multiple vendors into many different devices over the years, it's virtually impossible for a third party to track the affected products. The threat model under which this type of vulnerability is exploitable is the limiting factor for its actual impact.

In essence, any actor that can access the network traffic between the NVR and the end user, including the P2P third-party server provider in some scenarios, could access and view confidential A/V streams.

4.1.5 Verkada Security Camera Breach

While P2P vulnerabilities may or may not result in breaches and exposure of confidential information, in March of this year a very public security camera cyberattack occurred.

The affected vendor was Verkada and the outcome was that perpetrators gained access to the live video feeds of 150,000 surveillance cameras. Unauthorized viewing of images from inside hospitals, jails and manufacturing facilities brought home the risks involved in leveraging IoT devices for legitimate business purposes. Most of the victims of this attack only found out about it



when images of their facilities were shared over the internet.

Technical details provided by the vendor indicate the attackers gained access to an internet-exposed server used by Verkada's support team to carry out maintenance operations on customer cameras. Within this system, the intruders gained privileged account credentials that eventually allowed access to surveillance cameras deployed at thousands of customer sites.

In addition to acquiring the video streams, the attackers were able to execute shell commands on the breached cameras.⁵⁹ This is particularly worrisome because it's unlikely that all Verkada customers deployed the devices in a perfectly secured Zero Trust environment.

Although the vendor declared that all the shell commands issued through the internal tool were logged, from the point of view of a breached end user, this information might not be enough to investigate the situation. It's always difficult to predict what an



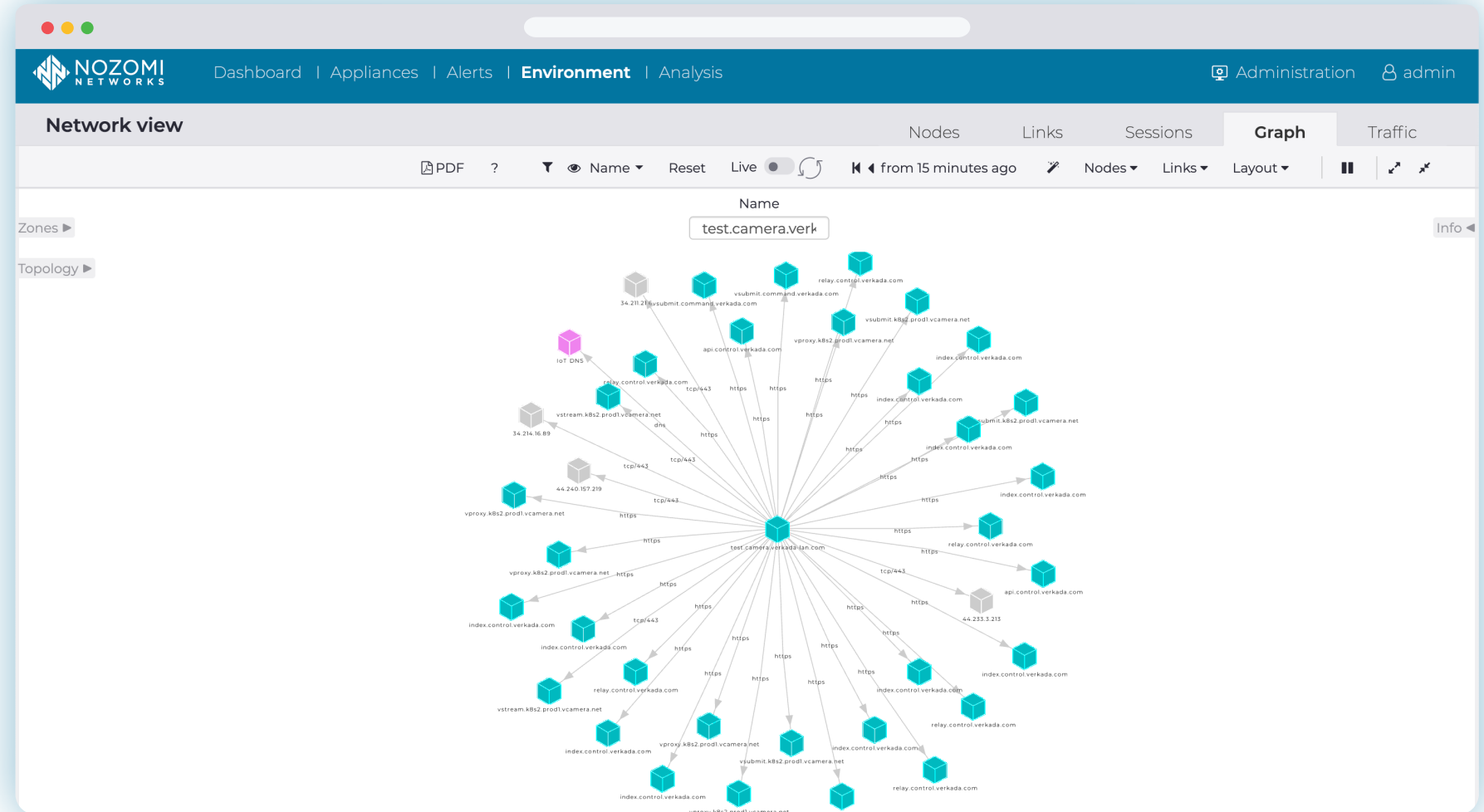
The Live Video Feeds of 150,000 Security Cameras were Exposed in the Verkada Cyberattack

Attackers were also able to execute shell commands on breached cameras, providing an entry point for lateral movement on victims' networks. **This could lead to consequences such as data theft, ransomware deployment or system disruption.**



advanced malicious actor, with a specific plan in mind, can come up with.

Furthermore, it's not uncommon for anybody with red team experience to prepare an engagement where the only entry point within an organization is represented by a shell on an IoT device. In these scenarios, a popular option is to upload the tools required for lateral movement on a third-party website, then download the tools and run them from the IoT device, based on the specific needs.



Testing of a Verkada D40 camera in the Nozomi Networks lab showed that it interacts with several external hosts for regular firmware updates, remote access to the video feed and maintenance operations.



4.2 Recommendations

4.2.1 Vendor and Security Camera Selection



Whether you're an organization in the critical infrastructure, manufacturing or government sector, or a

home user of security cameras, careful due diligence when purchasing security cameras is highly recommended.

If you want to take advantage of remote viewing of A/V streams, ask these questions:

- What measures has the vendor taken to ensure cybersecurity and data privacy?
- What technology is used to provide remote access? If a software component is involved, what is it and how secure is it?
- What is the reputation of the vendor(s)? What are their privacy policies?

- What is the jurisdiction of the vendor(s)? What laws are in place to ensure the confidentiality of your data?

Regarding security systems that use P2P functionality, only enable this functionality if the vendor can provide a thorough technical explanation of its design. How do they ensure that the algorithms used in their products are secure?

Overall, it's important to carefully evaluate the trade-offs between simple-to-use remote viewing capabilities, and the privacy and security risks of security camera systems.

4.2.2 Deploy Network Monitoring Before Deploying IoT Devices



Network monitoring is a foundational element of mature security programs for IT networks but is

mainly in the adoption phase for OT and IoT environments. It is especially important in these environments, however, as they are particularly lacking secure-by-design products and systems.

The functioning of IoT devices is often opaque, but monitoring their network behavior with anomaly detection provides much-needed alerts that highlight unusual behavior.

In the case of the Verkada cyberattack, for example, a network learning system would understand that communication with `api.control.verkada.com` and `index.control.verkada.com` over HTTPS is expected for this device and use that as a behavior baseline. If an attacker were to remotely access a shell running on the device through the vendor's interface, any action they then take would deviate from the established baseline, and be flagged as an alert.

With the goal of further compromising

the target network using the camera as a launchpad, an attacker would have to perform reconnaissance to better understand the target. This would involve activities such as port scanning or credential guessing against hosts inside the local network. Both are clear deviations from the device's established baseline behavior and would generate timely anomaly alerts.

Detecting post-infection nefarious activities is fairly trivial with network monitoring technologies like those from our company. And, it's important to recognize that today we're discussing Verkada, but tomorrow it will be a new vendor, and yesterday was a different attack.

Knowing that the threat of attack is constant, it's crucial to have independent and reliable cybersecurity monitoring technology already in place to manage the risks posed by IoT security cameras.



Furthermore, having monitoring in place before an incident happens can mean the difference between fully recovering, and not. If the response plan is simply to patch up the infected devices—without tracing the rest of the attackers' footsteps—you'll likely end up needing multiple remediations. The malicious code could still be in another part of the enterprise, and operators may have to disinfect and attempt to remove malicious code again.

Understanding the following is as important as identifying the initial actor vector:

- Reconnaissance activities: what the attackers searched for
- Lateral movement: where they navigated to
- Persistence: what other systems they may have breached
- Exfiltration: what data was compromised or downloaded

Not having these types of records severely impacts the recovery efforts.

In a Zero Trust model, using a cybersecurity monitoring system to watch for signs of infection could have reduced the impacts to some of Verkada's victims. For example, one publicly known victim became aware of their infection only after it was revealed in posts on Twitter. Had behavior monitoring and anomaly detection been in place, the company's cybersecurity team would have been alerted on initial connection attempts from the infected device. This would have provided them with the opportunity to respond before the attackers were able to do any further damage.



5

Conclusions

5.1 What You Need to Know to Fight Ransomware and IoT Vulnerabilities

35





5.1 What You Need to Know to Fight Ransomware and IoT Vulnerabilities

In a dynamic and escalating threat environment, this report highlights security risks in three threat areas. These are ransomware, new vulnerability disclosures and the security risks of IoT security cameras.

Understanding these risks and thinking through the consequences of your organization being attacked or exposed by them should help you re-evaluate your cybersecurity posture.

As ransomware and vulnerabilities proliferate, make sure your defenders have the tools they need. This includes real-time visibility of IT, OT and IoT assets and actionable threat and vulnerability information.

The Colonial Pipeline breach is a dramatic and instructive example of the significant risks of ransomware. While the OT network was not directly breached, pipeline systems were shut down for six days. This attack highlights the linkage that exists between IT and OT, even if the malware does not cross between systems.

We urge you to adopt a post-breach mindset, intensify your focus on cyber resiliency, and review your business continuity plans.

This includes making sure your security teams can act quickly if a breach occurs, and work hand-in-hand with other business groups for disaster recovery.

Vulnerability disclosures are on the rise and will continue to be a challenge for security teams.

Monitoring ICS-CERT advisories, prioritizing vulnerabilities and patching or mitigating to combat the top risks are a cornerstone of any industrial security program.

The post-pandemic economy is speeding up, increasing demands on critical infrastructure, manufacturing and demand across all sectors.

It's 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 IoT and OT systems, can lead to blind spots.



The overall cybersecurity market has realized that preventing all attacks is an unrealistic goal. Emphasis is shifting to detecting potential attacks and limiting intruders' ability to achieve their objectives if they gain access. The shift underway is toward a zero trust or deny-by-default security posture.⁶⁰



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](#)



6. References

1. **“When will the COVID-19 Pandemic End?”** Charumilind, S., Craven, M., Lamb, J., Sabow, A., & Wilson, M, McKinsey & Company, March 29, 2021.
2. **“Global Economic Prospects,”** The World Bank, June 8, 2021.
3. **“Already a Record-Breaking Year for Ransomware, 2021 May Just Be Warming Up,”** Wolff, A., SonicWall, June 21, 2021.
4. **“Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound,”** Coveware, April 26, 2021.
5. **“ICS-CERT Advisories,”** Department of Homeland Security.
6. **“2021 Manufacturing Industry Outlook,”** Wellener, P., Deloitte.
7. **“IoT Security Market by Type (Network Security & Cloud Security), Component, Solution (Identity and Access Management, Security Analytics, & Device Authentication & Management), Service, Application Area, and Region — Global Forecast to 2025,”** MarketsandMarkets, July 2020.
8. **“Ransomware and Critical Infrastructure,”** Jablanski, D., Kelly, M., Guidehouse Insights, 1Q 2021.
9. **“Already a Record-Breaking Year for Ransomware, 2021 May Just Be Warming Up,”** Wolff, A., SonicWall, June 21, 2021.
10. **“Panic buying strikes Southeastern United States as shuttered pipeline resumes operations,”** Englund, W., Nakashima, E., The Washington Post, May 12, 2021.
11. **“U.S. Pipeline Cyberattack Forces Closure,”** Eaton, C., Volz, D., The Wall Street Journal, May 8, 2021.
12. **“JBS cyberattack: From gas to meat, hackers are hitting the nation, and consumers, where it hurts,”** Rosenbaum, E., CNBC, June 2, 2021.
13. **“Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound,”** Coveware, April 26, 2021.
14. **“Global Ransomware Damage Costs Predicted To Reach \$20 Billion (USD) By 2021,”** Morgan, S., Cybercrime Magazine, October 21, 2019.
15. **“Ransomware World in 2021: Who, How and Why,”** Securelist, May 12, 2021.
16. **“Anatomy of Attack: Inside BazarBackdoor to Ryuk Ransomware ‘one’ Group via Cobalt Strike,”** Kremez, V., Advanced Intel, November 6, 2020.
17. **“Ransomware Kill Chain: Part 1: Why Ransomware Is Not A Typical Cyberattack,”** Hornetsecurity.
18. **“Ransomware: The True Cost to Business,”** Bezvershenko, L., Galov, D., Kwiatkowski, I., Cybereason, June 16, 2021.
19. **“The State of Ransomware 2021,”** Sophos, April 27, 2021.
20. **“Colonial Pipeline Ransomware Attack: Revealing How DarkSide Works,”** Kleymentov, A., Nozomi Networks, May 19, 2021.
21. **“Colonial Pipeline Hack Claimed by Russian Group DarkSide Spurs Emergency Order from White House,”** Collier, K., NBC News, May 10, 2021.
22. **“DarkSide Ransomware Has Netted Over \$90 million in Bitcoin,”** Elliptic, May 18, 2021.
23. **“The Moral Underground? Ransomware Operators Retreat After Colonial Pipeline Hack,”** Otto, G., Intel471, May 14, 2021.
24. **“Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,”** Department of Justice, Office of Public Affairs, June 7, 2021.
25. **“Computer giant Acer hit by \$50 million ransomware attack,”** Abrams, L., BleepingComputer, March 19, 2021.
26. **“Ransomware gang demands \$50 million from computer maker Acer,”** Cimpanu, C., The Record, March 19, 2021.
27. **“Apple supplier Quanta hit with \$50 million ransomware attack from REvil,”** Coombs, V., TechRepublic, April 21, 2021.
28. **“JBS Paid \$11 Million to Resolve Ransomware Attack,”** Bunge, J., The Wall Street Journal, June 9, 2021.



29. [“A Ransomware Attack Hit Up To 1,500 Businesses. A Cybersecurity Expert On What's Next,”](#) Fadel, L., NPR, July 6, 2021.
30. [“Latest ransomware attack appears to hit hundreds of American businesses,”](#) The Guardian, July 3, 2021
31. [“Kia Motors America Suffers Ransomware Attack, \\$20 Million Ransom,”](#) Abrams, L., BleepingComputer, February 17, 2021.
32. [“Computer giant Acer hit by \\$50 million ransomware attack,”](#) Abrams, L., BleepingComputer, March 19, 2021.
33. [“CNA Financial Paid \\$40 Million in Ransom After March Cyberattack,”](#) Mehrotra, K., Turton, W., Bloomberg, May 20, 2021.
34. [“Ransom Gangs Emailing Victim Customers for Leverage,”](#) Krebs, C., KrebsSecurity, April 5, 2021.
35. [“Apple Targeted In \\$50 Million Ransomware Hack of Supplier Quanta,”](#) Mehrotra, K., Bloomberg, April 20, 2021.
36. [“Colonial Pipeline Boss Confirms \\$4.4M Ransom Payment,”](#) BBC News, May 19, 2021.
37. [“Chemical distributor pays \\$4.4. million to DarkSide ransomware,”](#) Abrams, L., BleepingComputer, May 13, 2021.
38. [“Asia Division of Cyber Insurance Company Hit with Ransomware Attack,”](#) Greig, J., ZDNet, May 18, 2021.
39. [“Irish Cyber-Attack: Hackers Bail Out Irish Health Service for Free,”](#) BBC News, May 21, 2021.
40. [“JBS Paid \\$11 Million to Resolve Ransomware Attack,”](#) Bunge, J., The Wall Street Journal, June 9, 2021.
41. [“Zero Trust and its role in securing the new normal,”](#) Lin, J., Hines, C., Microsoft, May 26, 2020.
42. [“BeyondCorp,”](#) Google Cloud.
43. [“Responding to the Colonial Pipeline Breach & CISA Ransomware Alert,”](#) Capdevielle, E., Nozomi Networks, May 13, 2021.
44. [“Hackers hit Norsk Hydro with ransomware. The company responded with transparency,”](#) Briggs, B., Microsoft, December 16, 2019.
45. [“JBS Paid \\$11M to REvil Gang Even After Restoring Operations,”](#) Montalbano, E., ThreatPost, June 10, 2021.
46. [“ICS-CERT Advisories,”](#) Department of Homeland Security.
47. [“2021 Manufacturing Industry Outlook,”](#) Wellener, P., Deloitte.
48. [“ICS Advisory \(ICSA-21-131-04\): Siemens SINAMICS Medium Voltage Products Remove Access \(Update A\),”](#) Cybersecurity and Infrastructure Security Agency, June 8, 2021.
49. [“ICS Advisory \(ICSA-21-019-01\): dnsmasq by Simon Kelley \(Update A\),”](#) Cybersecurity and Infrastructure Security Agency, March 9, 2021.
50. [“ICS Advisory \(ICSA-20-203-01\): Wibu-Systems CodeMeter \(Update E\),”](#) Cybersecurity and Infrastructure Security Agency, February 11, 2021.
51. [“Talking About Cybersecurity Vulnerabilities in Medical Devices Shouldn't Be Taboo,”](#) Tamari, N., HIT Consultant Media, June 17, 2021.
52. [“Alert \(AA20-205A\): NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems,”](#) Cybersecurity and Infrastructure Security Agency, July 23, 2020.
53. [“Video Surveillance Market by System, Offering \(Hardware \(Camera, Storage Device, Monitor\), Software \(Video Analytics, Video Management System\) & Service \(VSaaS\)\), Vertical \(Commercial, Infrastructure, Residential\), and Geography - Global Forecast to 2025,”](#) MarketsandMarkets, April 2020.
54. [“Defending Against IoT Security Camera Hacks Like Verkada,”](#) Di Pinto, A., Nozomi Networks, March 12, 2021.
55. [“Security Cameras Vulnerable to Hijacking,”](#) Marrapese, P., Hacked.camera.
56. [“New Reolink P2P Vulnerabilities Show IoT Security Camera Risks,”](#) Di Pinto, A., Nozomi Networks, January 19, 2021.
57. [“Cloud Platform Solution for Transmission Efficiency and Data Security,”](#) Throughtek.
58. [“New IoT Security Risk: ThroughTek Supply Chain Vulnerability,”](#) Nozomi Networks Labs, June 15, 2021.
59. [“Defending Against IoT Security Camera Hacks Like Verkada,”](#) Di Pinto, A., Nozomi Networks, March 12, 2021.
60. [“Ransomware and Critical Infrastructure,”](#) Jablanski, D., Kelly, M., Guidehouse Insights, 1Q 2021.



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.

© 2021 Nozomi Networks, Inc.

All Rights Reserved.

NN-SEC-RP-FULL-2021-1H-001

<https://t.me/learningnets>

nozominetworks.com