NOZOMI NETWORKS

What You Need to Know to Fight Ransomware and IoT Vulnerabilities

Including Recommendations for Enhancing Cyber Resilience

EXECUTIVE SUMMARY

OT/IoT Security Report

July 2021

Ransomware Attacks Result in Operational Disruption

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 year[3] 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.

Ransomware Attacks Are Sophisticated

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.

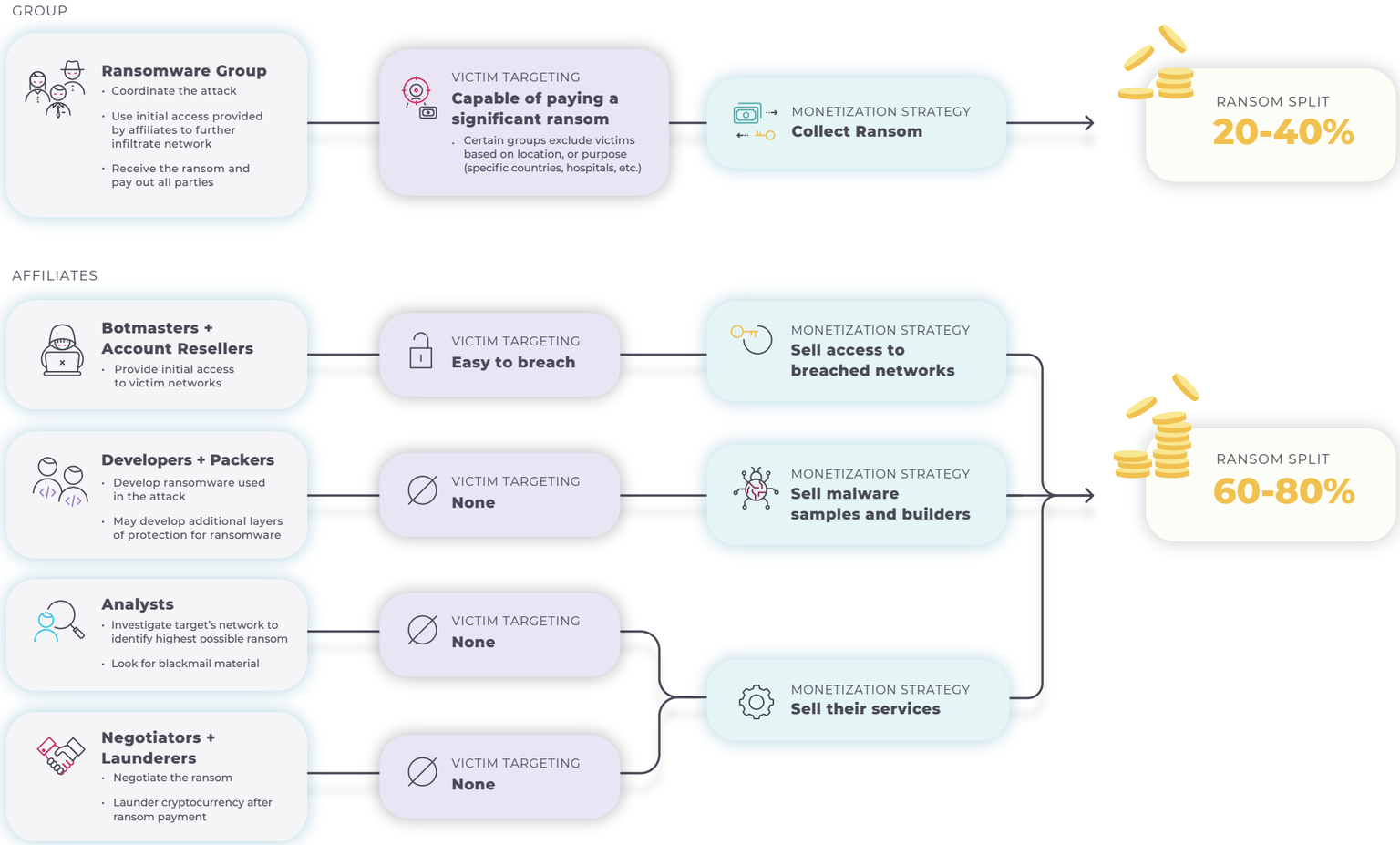
Nozomi Networks Labs studied the internals of the DarkSide executable and revealed the malware's techniques in three areas:

- 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



Critical Manufacturing Vulnerabilities Are on the Rise

Vulnerability Research

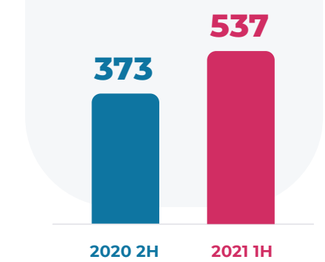
Vulnerabilities published by ICS-CERT[5] increased 44% in the first half of 2021 as compared to the second half of 2020. While the number of vendors affected rose by just 5%, the number of products rose 19%.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

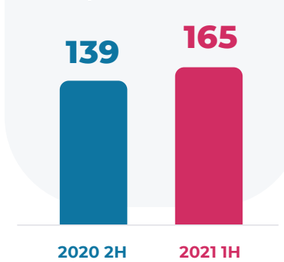
The top three industries affected include Critical Manufacturing, a grouping identified as Multiple Industries, and Energy. The key industry trend is that vulnerabilities solely affecting the Critical Manufacturing sector rose by 148%. This poses an additional challenge to an industry where many segments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

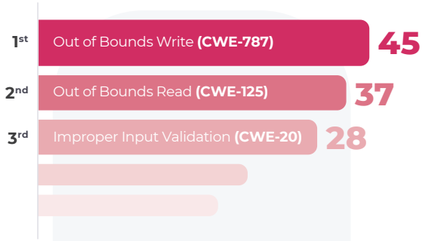
ICS Vulnerability Trends

+44% increase
in the **total number of vulnerabilities** disclosed

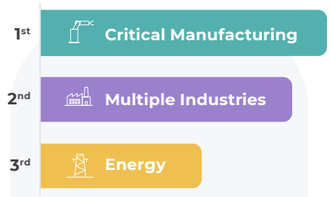


+19% increase
in the actual number of **products affected**

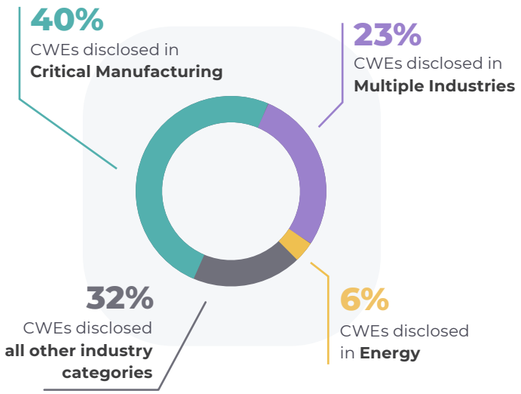




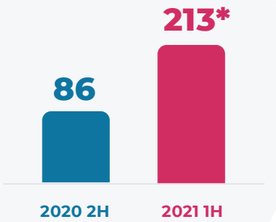
Most-disclosed CWEs
Compared to 2020 2H, CWE-787 had a +64% increase, while CWE-125 and CWE-20 each dropped down one place.



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



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



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.*

Insecure IoT Security Cameras Are a Growing Concern

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 a of 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.

VIDEO SURVEILLANCE MARKET SIZE GROWTH EXPECTATION

From **US $45.5 billion** in 2020 › to **US $74.6 billion** by 2025

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.**

What You Need to Know to Fight Today's Threats

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.

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

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.

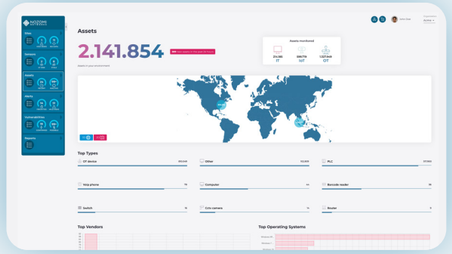
Continuous advancement of your IT/OT security posture is the best way to ensure the availability, safety and confidentiality of your operational systems.

Improve Operational Resilience with OT/IoT Visibility & Security

Download the full report for:

- Ransomware insights
- Vulnerability analysis
- IoT security camera risks
- Recommendations

Download



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

Table of Contents for the Full Research Report

1. Executive Summary 4

2. Ransomware Insights 9

2.1 Introduction 10

2.1.1 Ransomware as a Service (RaaS) 10

2.1.2 The RaaS Ecosystem 11

2.1.3 Ryuk and the Ransomware Kill Chain 12

2.1.4 Automated Attack Execution 12

2.2 Notable Ransomware Attacks 13

2.2.1 DarkSide Attack on Colonial Pipeline 13

2.2.2 REvil Attack on JBS Foods and Others 14

2.2.3 Timeline of Notable Year-to-Date Ransomware Attacks 15

2.3 Recommendations 16

2.3.1 Malware Infection Prevention 16

2.3.2 OT Network Monitoring 16

2.3.3 Network Segmentation 16

2.3.4 Threat Intelligence 16

2.3.5 Secure Remote Access 16

2.3.6 Adopting a Post-Breach Mindset 17

2.3.7 Disaster Recovery Planning 17

3. Vulnerability Analysis 18

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

4. IoT Security Camera Spotlight 24

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

5. Conclusions 34

5.1 What You Need to Know to Fight Ransomware and IoT Vulnerabilities 35

6. References 37

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.

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-ES-2021-1H-001

nozominetworks.com