NOZOMI NETWORKS LABS

Trends and Countermeasures for Critical Infrastructure Attacks

How to Shore Up Cyber Defenses in OT/IoT Environments

EXECUTIVE SUMMARY

OT/IoT Security Report

2021 2H Review

Ransomware Attacks Are Causing Operational Disruption

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

Supply Chain Attacks Are Spreading Damage Quickly

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.

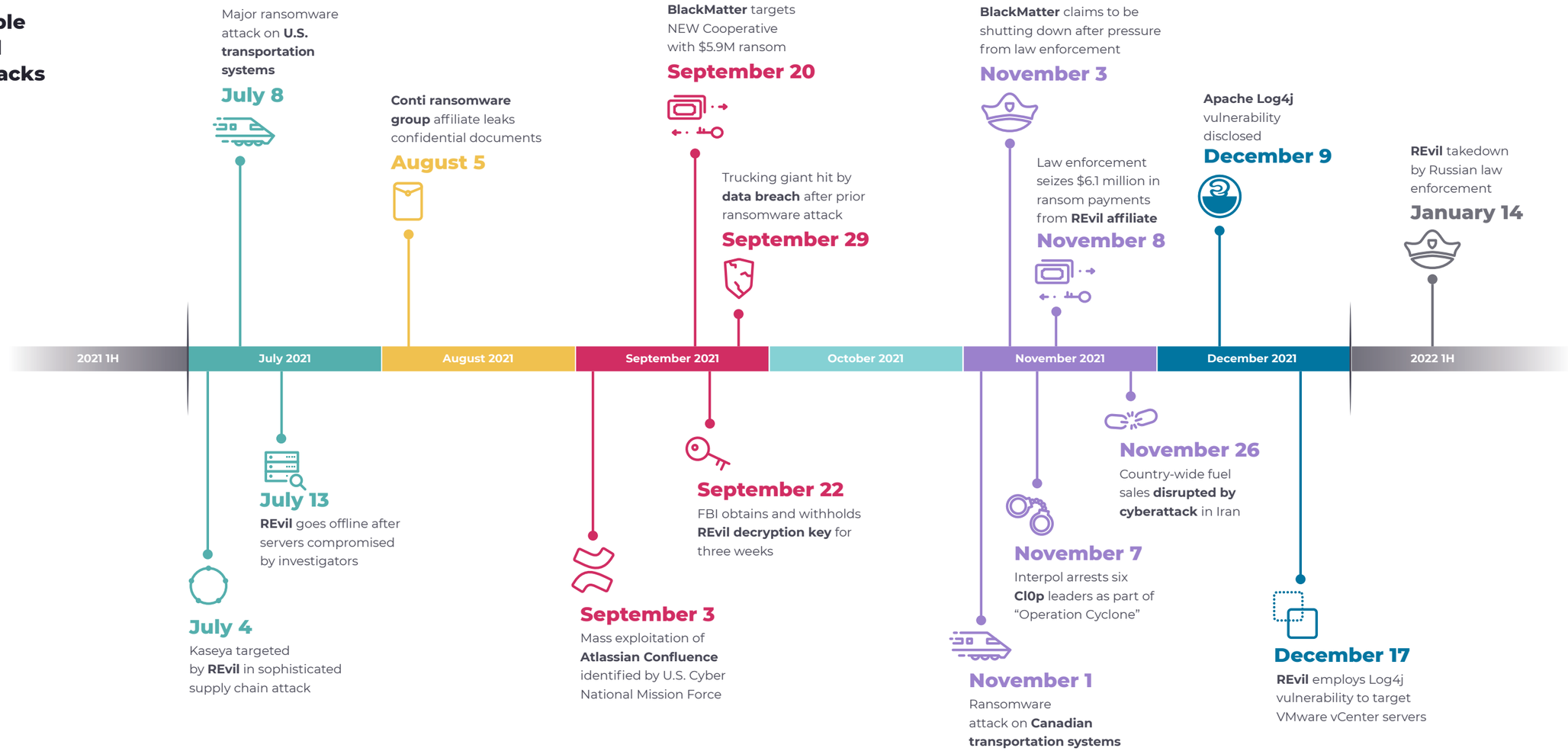
When vulnerabilities are announced in open-source software, which can be used by many applications, the damage can be just as, or even more, extensive than single-vendor software. It depends on how widely used the library component is.

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 OT/IoT Vulnerability Research

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

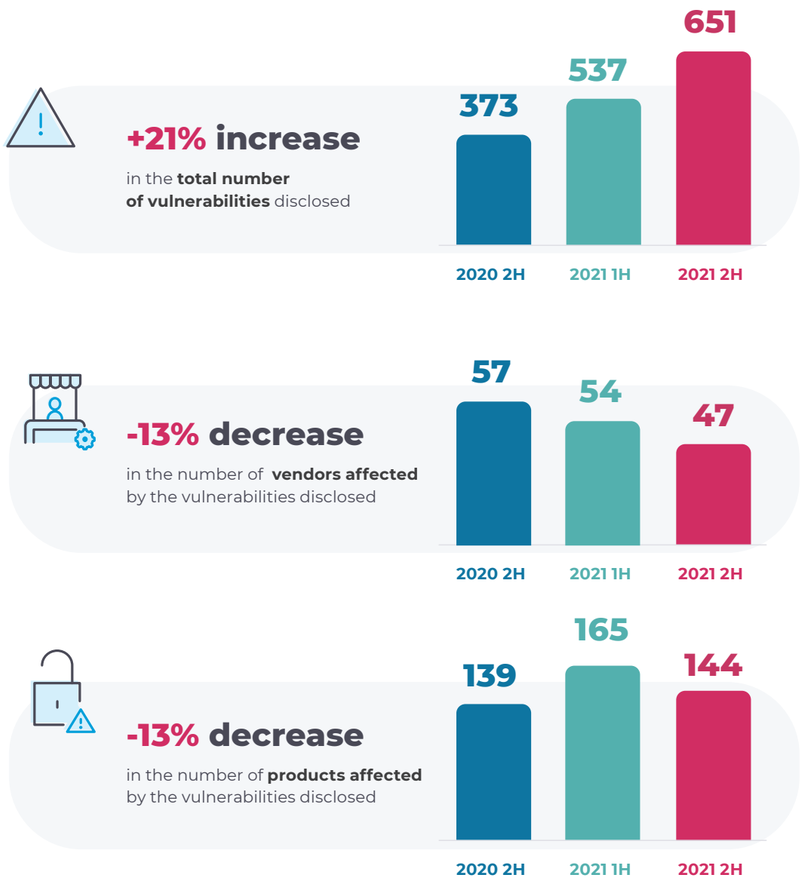
OT and IoT devices are the primary research area for Nozomi Networks Labs. In the last several years, IoT devices have become a common entry point to the entire network and are often overlooked compared to widely deployed IT platforms and operating systems.

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



What You Need to Know to Fight Today's Threats

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.

More OT/IoT Cybersecurity Research from Nozomi Networks Labs

RESEARCH REPORT

OT/IoT Security Report: Trends and Countermeasures for Critical Infrastructure Attacks

Download the full report for:

- Insights on ransomware and software supply chain attacks in 2021 2H
- OT/IoT vulnerability research and exploitation trends
- Suggested remediation strategies

Download

WHITE PAPER

The S3CUREC4M Project: Vulnerability Research in Modern IP Video Surveillance Technologies

Download the white paper for:

- Hardware analysis and firmware extraction techniques
- Insight into the software attack surfaces in surveillance systems
- Security assessments of modern IP video surveillance technologies

Download

Table of Contents for the Full Research Report

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-2021-2H-001

nozominetworks.com