NOZOMI NETWORKS | bako tech®

Protect Your Operations with New OT/IoT Security Threat Insights

Including Recommendations for Enhancing Cyber Resilience

EXECUTIVE SUMMARY

OT/IoT Security Report

February 2021

www.bakotech.com

Supply Chain Threats Reach New Heights

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

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

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

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

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

Supply Chain Threats and Vulnerabilities

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

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

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

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

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

Ransomware Dominates the Threat Landscape

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

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

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

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

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

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

Ransomware

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

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

Ryuk's cyber kill chain includes:

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

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

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

Ransomware is the second most notable threat category.

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

Nation State and Ransomware Threat Groups Are Targeting Healthcare

Other Notable Threats

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

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

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

IoT IS AN EASY AND PLENTIFUL TARGET FOR ATTACKERS

98% of all IoT device traffic is unencrypted

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

Vulnerability Trends

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

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

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

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

IoT Security Guidelines

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

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

Evaluate Defenses Against the Emerging Threat Landscape

Recommendations

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

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

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

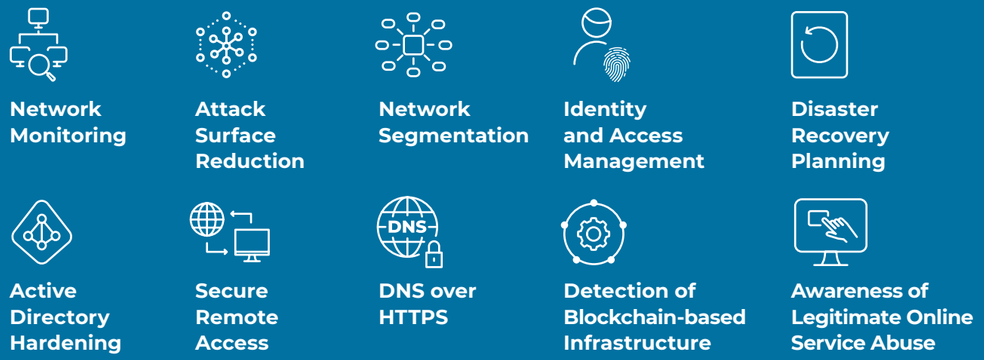
- Network Monitoring
- Attack Surface Reduction
- Network Segmentation
- Identity and Access Management
- Disaster Recovery Planning
- Active Directory Hardening
- Secure Remote Access
- DNS over HTTPS
- Detection of Blockchain-based Infrastructure
- Awareness of Legitimate Online Service Abuse

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

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

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

10 ACTIONABLE INSIGHTS



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

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

NOZOMI NETWORKS

BAKOTECH

True Value-Added IT-Distribution

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. Geographically the Group operates in 26 countries covering Central and Eastern Europe, the Balkans, the Baltic States, the Caucasus, Central Asia with offices in Prague, Krakow, Riga, Kyiv, Baku and Nur-Sultan.
BAKOTECH is the official distributor of Nozomi Networks in Ukraine, Belarus, Azerbaijan, Georgia, Kazakhstan, Uzbekistan, Turkmenistan, Tajikistan, Kyrgyzstan.

More information: www.bakotech.com, **nozomi@bakotech.com.**

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

www.bakotech.com