NTT GLOBAL THREAT INTELLIGENCE CENTER

Monthly Threat Report

January 2020

Contents

Cybersecurity for Industrial Control Systems (ICS)

Lead Analyst: Zhanwei Chan — Global OT/IoT Practice Director

Analysts and consultants from NTT Ltd. have spoken to hundreds of organizations operating Industrial Controls Systems (ICS). Operational Technology (OT) is becoming progressively intertwined with Information Technology (IT). Apart from the nuclear sector, true air-gapped OT networks have started to slowly disappear.

A main driver for this connectivity is Industry 4.0 (in the manufacturing sector), smart maintenance and monitoring (in the utilities sector), and remote monitoring and control (in smart spaces like smart cities and smart buildings).

Majority of attacks on OT come from IT

We have seen time and time again how a cyberattack incident crosses from a traditional IT environment over to an OT environment. The first of its kind, the Ukraine power plant attack in 2015 and the more recent attack on a U.S. Maritime Transportation Security Act (MTSA)-regulated facility in late 2019, are both believed to have originated via the IT email system. Both of these attacks were intended to disrupt mission operations of an Industrial Control System OT environment and were born out of the traditional IT environment.

Despite these well-publicized cases, it is concerning that there are still organizations which have insufficient protection against such malware.

Malware can be complex – obfuscation techniques and fileless malware help ensure that no single antivirus solution is effective at catching all malware. As a result, many organizations remain at risk.

More sinister attacks to come

In 2019, our Global Threat Intelligence Report indicated that 47% of hostile activity directed at manufacturing clients was related to reconnaissance. Reconnaissance is the initial stage used by attackers to understand the security of a system. It should not be surprising, then, that as knowledge of OT environments improves, as attacks develop and as implementations spread, we see more attacks attempted in the future.

NTT Ltd. analysts have met with critical infrastructure organizations which have not been able to successfully engage their IT and OT teams to collaborate to protect their ICS network. Without action to secure their environments now, these organizations are likely to continue being exposed to potential attacks.

Malware can be complex – no single antivirus solution is effective at catching all malware.

Issues preventing OT from being properly secured

Throughout client discussions, NTT Ltd. has identified several common challenges faced by a CIO/CISO when securing the OT network:

1. One of the most consistent challenges has been that, while cybersecurity may be part of the IT team, the IT team does not have comprehensive knowledge of the OT network. This creates a gap in understanding within the organization's cybersecurity team on how to secure the OT network.
2. Another common issue is the lack of solutions designed to effectively secure the OT network. Common IT cybersecurity tools have historically been implemented to operate within an IT environment and may not function correctly in an OT environment. These same IT cybersecurity tools can be intrusive and have a high probability of disrupting ICS systems.
3. A third common issue is lack of process and capabilities to deal with known risks. For example, implementing a security patch not approved by the ICS vendor.
4. Finally, many OT systems do not offer support for multiple users. Some OT systems simply do not support multiple usernames which can complicate support and operations, as well as lead to inappropriate levels of password sharing.

Cybersecurity for Industrial Control Systems (ICS), continued

Global trends in OT cybersecurity

Based on analysis of NTT Ltd. engagements and interactions with clients and potential clients, we have identified that:

- 42% of OT organizations start their OT cybersecurity journey by carrying out an initial discovery assessment.
- 69% of OT organizations are taking the opportunity to deploy some form of OT Threat Detection (e.g. OT-Intrusion Protection and Detection). These OT-IDS tools are used to passively discover the OT network in the previous point.
- 20% of OT organizations are upgrading their industrial firewalls to Next Generation Firewall (NGFW). This can provide valuable granularity and can differentiate between bad or good actions. NGFW also comes with the ability to detect new threats when combined with appropriate use of accurate and timely threat intelligence.
- Only 2% of OT organizations have started to upgrade and implement Next Generation Endpoint Security (e.g. Next Generation AV, Dynamic Application Whitelisting & Control, etc.). These endpoint security controls can be extremely effective in stopping malware on endpoints, and we expect this percentage to rise significantly.
- For OT organizations which have multiple autonomous facilities, the general approach appears to be creating a standardized reference architecture. This standard, unified architecture is then rolled out to individual facilities.

Other interesting approaches

NTT Ltd. also identified several innovative approaches to securing OT assets. While not all these techniques have been successful, two interesting options organizations may consider are:

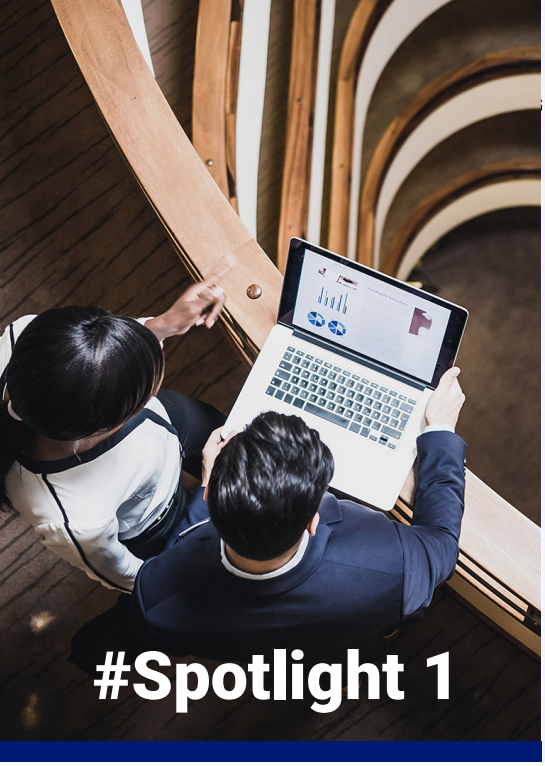
1. Take a risk-score approach to addressing OT Cybersecurity.
   The OT organization assigns a risk score to each network, system, endpoint and programmable logic controller. This score is influenced by security patches installed, if OS hardening carried out, and how critical the asset is to the OT process.
   All high-risk activities – such as remote access – are influenced by this risk score. The higher the risk score for any asset, the more vetting is given to any access to or by that asset.
2. Limit OT connections between systems to the same vendor.
   Vendor A is only allowed to connect to assets made by Vendor A. Vendor B can only connect to assets manufactured by Vendor B. In a well-defined environment, this can add a layer of control over network communications.

Technical recommendations

OT Cybersecurity can be difficult and may take years to fully implement. However, we understand that organizations need to implement some form of security quickly. While our strategic approach relies on a more asset and risk-driven approach, our general technical approach to securing OT network is:

1. Implement at least minimal protection and detection capabilities. For example, use OT-IDS to detect and monitor threats in the OT environment, and NGFW to isolate and stop any detected threats.
2. Operationalize and make full use of the OT-IDS Threat Detection and NGFW implementations, making sure both IT and OT are properly secured.
3. Implement advanced controls like Endpoint Security and Secure Remote Access.

OT Cybersecurity can be difficult and may take years to fully implement. We understand that **organizations need to implement some form of security quickly**, and can provide the strategic approach necessary to start securing their operations.



#Spotlight 1

Top 3 recommendations to protect your OT environment

Lead analyst: Tim Ennis — Senior Operational Technology Consultant

High-profile attacks on Industrial Control Systems (ICS)/Operational Technology (OT) and the implementation of regulations has led many organizations to actively work on improving their OT security.

However, there remain significant challenges to many organizations trying to assess risk in OT environments — in meaningful business terms — and to implement OT security solutions.

These remain the top three recommendations to improve OT security:

1. **Gain visibility into OT networks.**
   Validate that design documentation and asset inventories are up to date. If an inventory doesn't exist, create one using passive asset discovery techniques to understand the type of assets, their status, how they are connected and which protocols are being used.
   This enables key objectives such as performing OT risk assessment, implementing segmentation and understanding potential attack vectors such as uncontrolled remote access.
2. **Create a secure OT architecture.**
   Separate the OT network from the enterprise and external networks. Create security zones, prioritizing the most critical systems and ensure communication between zones is restricted to limited, defined, and monitored types of communication.
   Create a management system to provide governance and continuous improvement for OT systems, including documenting known configurations, procedures for controlling modifications, and system restoration.
   Use knowledge gained from visibility and risk assessments to develop options for implementing controls and prioritize the implementation of those which are most effective in reducing identified risk. Among other controls, this includes patch management, access control, whitelisting, endpoint detection and response (EDR), device hardening and anomaly detection.
3. **Exercise your controls.**
   Regularly perform incident response exercises to test organizational effectiveness in managing an incident. Start with the basics by performing a tabletop exercise to create or reinforce the correct roles within teams, using a range of skills across the organization (operations, IT, security, engineering and others).
   Test the ability to restart processes by using system and configuration backups, and check to ensure that any third-party support contracts are adequate in terms of response time and assistance provisions.
   Perform a structured assessment of systems to simulate the types of techniques which are known to be used by adversaries, such as the recently released MITRE ICS ATT&CK framework.

Tensions with Iran:
Is cyberwarfare looming?

Lead analyst: Jeannette Dickens-Hale — Senior All Source Threat Intelligence Analyst

On 3 January 2020, an American MQ-9 Reaper drone fired missiles into a caravan leaving Baghdad International Airport, killing Qassem Suleimani, Iran's head of the Islamic Revolutionary Guard Corps Quds Force (IRCG-QF), a U.S.-designated terrorist organization. Abu Mahdi al-Muhandis, leader of the Iran-backed Shiite militia, was also killed in the drone strike. Abu Mahdi al-Muhandis was responsible for the assault on the U.S. Embassy in Iraq on 31 December 2019. The attack was carried out by Hashed al-Shaabi, a pro-Iranian paramilitary group.

On 8 January 2020, in retaliation to the drone strike, Iran fired ballistic missiles at two U.S. bases in Iraq — Erbil base in northern Iraq and al-Asad Airbase in western Iraq. Several ballistic missiles struck al-Asad, one missile struck Erbil. During the Iranian missile attacks against U.S. forces based in Iraq, Ukraine International Airlines Flight PS752 was shot down.

After initial denials, Iran admitted they had unintentionally shot down the plane, killing all 176 passengers and crew aboard.

In addition to the missile strikes against U.S. bases in Iraq, Iranian cyberattacks could be another method of retaliatory attack. Iran stated that the U.S. would face retaliation, leading to the widespread expectation that this reaction, in part, would take place in the form of cyberwarfare. Iran increased their offensive cyberattack capabilities and, based on historical attack vectors, could increase cyberattacks against the critical infrastructure of the U.S. and their allies.

Historically, Iranian Advanced Persistent Threats (APT) tactics, techniques and procedures (TTPs) include leveraging wiper malware, credential dumping, obfuscated files or information, data compression, user execution, scripting, registry run keys/startup folder, remote file copy, spear-phishing links and spear-phishing attachments.

Since the drone strike killing Qassem Suleimani on 8 January 2020, Iranian hackers increased their probing and reconnaissance activities. The FBI alerted U.S. companies that cleared defense contractors, government agencies, academia and nongovernmental organizations focusing on Iran issues could be potential Iranian cyberattack targets. The FBI alert mentioned no Iranian breaches of networks as part of that activity.

To date, NTT Ltd.'s GTIC analysts have identified activity and malware sourcing from Iran, but this activity has not deviated significantly from activity which is normally expected. That does not mean there is no danger in escalation, and GTIC analysts recommend the following best practices for incident preparation and mitigation:

- Disable unnecessary ports and protocols.
- Enhance monitoring of network and email traffic.
- Patch externally facing equipment.
- Log and limit usage of PowerShell.
- Ensure backups are up to date.

For further details on incident preparation and attack mitigation strategies, please see the U.S. CERT advisory aa20-006a[1].

Additionally, GTIC analysts recommend following the MITRE ATT&CK Framework[2] to further detect and mitigate Iranian advanced persistent threat (APT) techniques in the public domain.

[1] https://www.us-cert.gov/ncas/alerts/aa20-006a

[2] https://attack.mitre.org/.

NTT's Global Threat Intelligence Center

The NTT Security Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT Ltd. to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics, and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT Ltd's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2019 Global Threat Intelligence Report

This year's report focuses on several security challenges we have observed in organizations over the past year. Our analysis shows an escalation in coin mining, web-based attacks, and credential theft, along with changes in the sectors most targeted.

Download report

Risk:Value 2019

In 2019, 33 percent of organizations around the world would consider paying a ransom to a hacker rather than investing more in cybersecurity because paying the ransom is cheaper. Read more about this and other trends in the 2019 Risk:Value report.

Download report


NTT