Global Threat Intelligence Center

Monthly Threat Report

July 2021

Contents

Why did attacks targeting manufacturing increase so much in 2020?

Lead Analyst: Jon Heimerl, CISSP, Sr. Manager,
Global Threat Intelligence Center, US

Analysis for the NTT 2021 Global Threat Intelligence Report (GTIR) revealed that attacks targeting the manufacturing industry increased nearly 300% in 2020 over the volume from the previous year, accounting for 22% of all attacks.

An increase approaching 300% is a significant shift in attacks and paints a complex picture of attackers targeting manufacturing, since no single factor dominated this shift.

To add a little context, manufacturing has been a consistent target of hostile threat actors for years. Manufacturing has been in the top five targeted industries in seven of the past nine years. Many things change over nine years, but data indicates a consistent state of targeting – hostile threat actors have decided that manufacturing is an attractive target.

A more complex supply chain

Over those nine years, business and technology have changed dramatically. Manufacturing had to adapt to those changes while remaining cost-competitive. Many manufacturing organizations have adapted to more aggressive management of their supply chains to improve efficiencies and reduce costs. As a result, supply chains at manufacturing organizations have continued to grow more complex. Just-in-time manufacturing requires strong management of potentially complex supply chains. Manufacturing organizations often retain multiple suppliers to support lower-cost options while managing alternate sources to meet changing supply and demand dynamics. These demands mean manufacturing organizations have tended to develop supply chains that are more complex than many other industries. And, 'more complex' can also mean 'more sensitive to disruption.' A downstream attack or outage can have a dramatic effect on production capabilities.

Hence the need for manufacturing to establish and maintain business-to-business marketplaces, vendor/supplier programs, incentive programs, active order management systems, and other technologies designed to help manufacturing organizations manage their supply chains.

When manufacturing organizations manage complicated vendor/supplier/buyer relationships via online portals, those web-enabled portals are under attack with the increase observed in web application and application-specific attacks. If an organization manages these communications via email, all associated staff are more vulnerable to email spoofing and phishing attacks, increasing malware incidents. If an organization manages these communications via telephone, it can increase staff exposure to social engineering, along with associated increases in business email compromise, malicious phishing websites, and resultant malware.

Manufacturing 4.0

In its simplest form, Manufacturing 4.0 refers to the automation of manufacturing through smart technologies. This includes implementation of Operational Technology (OT), Internet of Things (IoT), and information and communications technology (ICT). This technology aims to automate operations, monitoring, and management of manufacturing systems to improve the efficiency of operations. Such operations have the potential to unlock significant competitive advantages, along with more timely and accurate information about how well diverse systems are operating. The accelerated adoption of IoT/OT has created a surge in the introduction of new technologies. But organizations have not been effectively leveraging solutions to optimize security.

These technologies also bring with them threats that attackers are explicitly directing at OT systems. Attacks against OT devices have continued to increase as attacks become even more automated, including implementation into botnets like Mirai. In addition, attackers regularly scan for exposed OT-related systems, to target immediately, or track for potential future targeting.

Increased complexity

One of the side effects of the demand put on manufacturing is a resulting increase in complexity of operations. Collaboration and supply-chain management tools result in an increased web presence for manufacturing organizations. Implementing additional OT and related networks results in more complex network infrastructures, and potentially more exposed systems. The increase in web-enabled applications and exposed systems means hostile threat actors have more targets to attack.

While manufacturing has not historically been the industry with the least mature security program, with a Cybersecurity Advisory benchmark maturity score of 1.21, their measured maturity is on the lower end of the scale. Furthermore, that maturity has been falling consistently over the past several years (1.45 in 2018, 1.32 in 2019, and 1.21 in 2020). Manufacturing is the only industry analysed for the 2021 GTIR that showed three years of decreasing security maturity. The assessment results suggest manufacturing as an industry has a hard time keeping up with changing security requirements associated with evolving environments.

There is some evidence of this in Application Security testing performed by NTT's WhiteHat Security during 2020, as reported in the 2021 GTIR.

Of the major industries analysed for the 2021 GTIR, manufacturing showed the highest number of vulnerabilities, with an average of 8.79 per site. These numbers indicate manufacturing is more vulnerable to attack, because, as an industry, their sites tend to have more vulnerabilities to other industries. The more vulnerabilities an organization's site has, the more exposed they are to attack from hostile threat actors.

Increased targeting

The problems facing manufacturing are complex, as is the reality of their increasing attack volume.

Supply-chain and OT-related demands are making manufacturing environments more complex and vulnerable. As a result, implementations are resulting in increased numbers of exposed vulnerabilities, while manufacturing's security maturity is falling.

Ultimately, the increase in attack volume targeting manufacturing is due to a variety of conditions. Some are listed above, but manufacturing also faces many of the same challenges as other industries, including ongoing support of a distributed work environment, shortages of qualified staff, and evolving regulatory requirements.

In closing, hostile threat actors have decided manufacturing is an attractive target industry, and they have developed automated tools and malware to help target the technology manufacturing is using.

OT Backup and Restore: Top three priorities

Lead Analyst: Jurgen Sanders, OT Security Consultant, Belgium

When implementing an Industrial Control System, cybersecurity may not be the highest priority component. However, organizations simply cannot skip some key cybersecurity elements when considering cyber incidents in production environments.

For instance, it is crucial to have accurate backups available that the organization can restore in the shortest time possible. IT methodologies and policies provide a foundation to backup and restore strategies in OT security. Still, due to the nature of OT environments, it's necessary to consider the unique aspects of OT and define additional measures when designing OT backup and restore policies. This short article aims to provide the reader with a list of three top priorities as initial guidance to start the journey of OT backup and restoration.

What to backup and when

As OT security professionals will acknowledge, having an up-to-date inventory of the OT environment will always be of tremendous value. The inventory, both from a hardware and software perspective, helps guide the organization to answer the question 'What parts of my production environment do I need to include in backups?' Knowing what to backup is a 'must-have,' and while it should seem evident in IT, it's less trivial in OT. Today, great tools are available to assist with asset discovery and detection. Proper tools help indicate patching requirements and provide guidance on the timing and frequency of backups, based upon discovered vulnerabilities.

Organizations must consider risk as a driving factor when setting priorities for backup. For example, the location of assets within the security architecture, such as more exposed versus less exposed assets (i.e., islands of automation versus highly connected assets), more valuable versus less valuable assets, more dynamic versus more static assets, in combination with a risk analysis will provide good inputs to the discussion about backup timing and frequencies for your OT assets.

OT/ICS backup and restore technology

In addition to the wide range of IT backup and restore technologies, it's valuable for organizations to consider specific tools and technology to aid in OT asset management. Organizations may or may not integrate those tools with an IT asset discovery and detection platform. Having an integrated solution will provide for more accurate asset discovery whilst providing backup availability, health and status reporting.

In addition to technologies, organizations must evaluate IT/OT security architecture when considering backup and restore capabilities. For example, will OT backups reside on both the OT and the IT sides? How will the organization securely transfer the backup and restore archives from IT to OT and vice versa? And, perhaps most importantly, what is the emergency recovery/restoration procedure in the event of an OT cyber incident when IT and OT systems may be compromised?

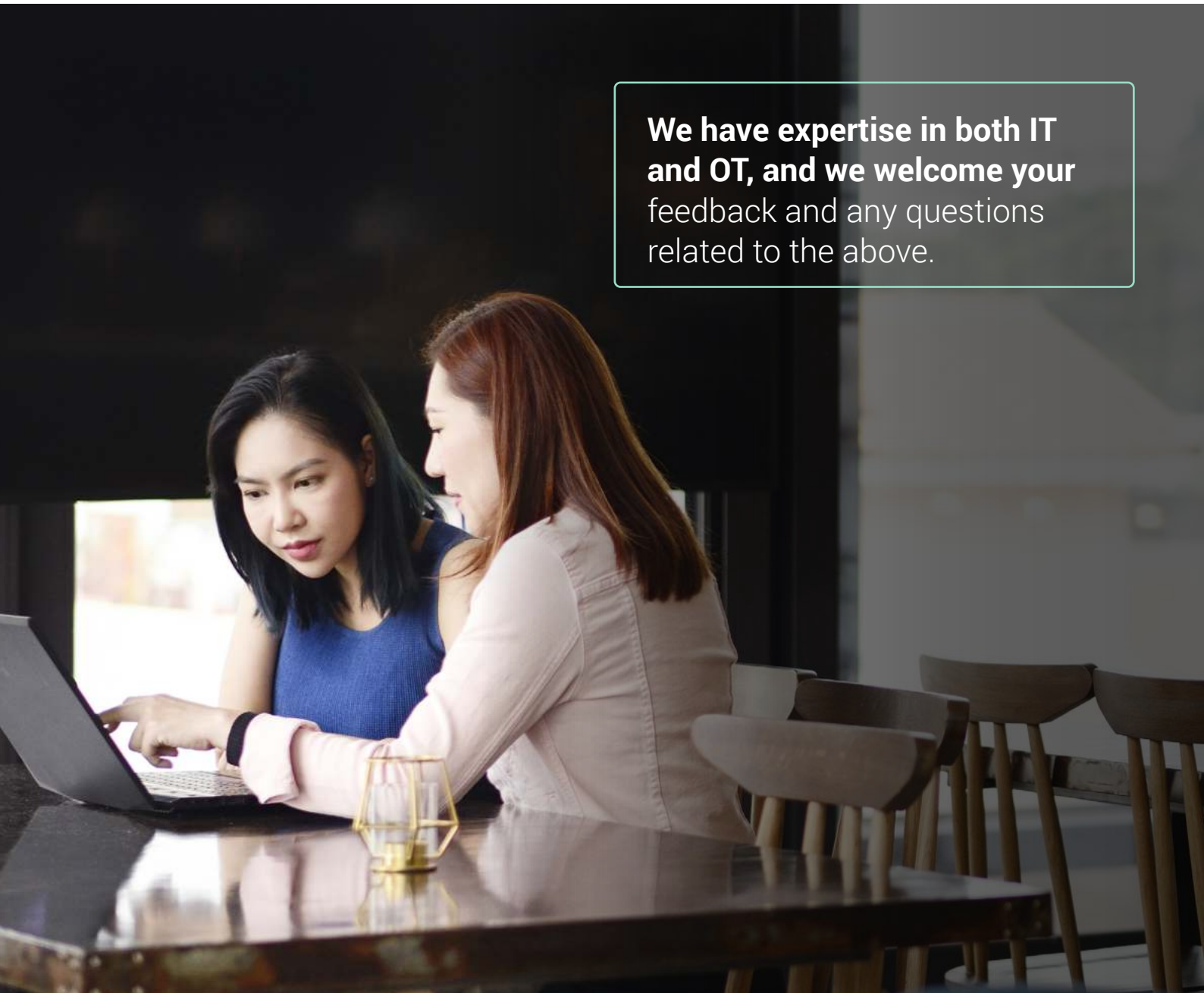
Having an up-to-date inventory of the OT environment will always be of tremendous value.

The dynamic aspect of OT

Because OT environments can be dynamic, it is even more crucial to consider OT backup and restoration. When restoring backups, organizations need to evaluate how to ensure the latest operating parameters of the machine or production line are applied to ensure the proper throughput, quality, etc. Often these operating parameters are stored in several locations: within the control system, within standard operating procedures, and often within people's brains. Next to traditional backup and restore functionalities, an organization should research how to backup and restore the dynamic elements of an OT operation. In a perfect world, all operating configurations are accurately stored in system memory and documented in up-to-date procedure guides. And while that perfect world is rare, innovative technology may give some answers here: organizations can evaluate if they can capture the years of experience of an operator into updated standard operating procedures and work instructions (i.e., through the use of smart glasses).

Summary

In summary, these three priorities will help provide guidance when designing robust incident response plans in industrial environments. NTT has expertise in both IT and OT, and we welcome your feedback and any questions related to the above or any other OT security challenges you may have.



NTT looks at Grim Spider's delicate web and Winnti Group's infrastructure

Lead Analyst: Jeremy Bender, Security Intelligence Writer, Global Threat Intelligence Center, US

NTT research teams, including NTT's Global Threat Intelligence Center (GTIC), regularly analyse threat groups and their infrastructure. By leveraging NTT's owned and operated global tier-1 IP backbones, correlation of data from targeted customers, internal research, and open-source intelligence (OSINT), we research new, emerging, and high capability threats.

Among the many cybercriminal groups we follow, the activities of Grim Spider (also known as FIN6 or UNC1878), which is part of the larger threat actor group Wizard Spider, and the Winnti Group, stand out due to their capabilities and operational tempo. We've recently released whitepapers on both groups.

Wizard Spider is known for its operation and deployment of the trickbot banking trojan. The trickbot infection chain can also include a final stage infection with Ryuk ransomware; Grim Spider is responsible for the deployment and operation of Ryuk in such attacks. Wizard Spider and Grim Spider's targeting predominantly appears indiscriminate; however, GTIC observed in NTT's 2021 Global Threat Intelligence Report (GTIR) that trickbot primarily targeted the finance and healthcare industries last year. Please find NTT's 2021 GTIR here.

As part of the threat research GTIC conducts, analysts reviewed a report from The DFIR Report titled 'Bazar Drops the Anchor.' The report included details about the IP address 23[.]94[.]51[.]80, which accessed a honey document during an incident response engagement. Using our global network visibility, analysts pivoted off the IP address to discover one of the threat actor's working environment nodes. GTIC associated the IP address and associated attack activity with the group Grim Spider.

By pivoting off the IP address, GTIC identified sites the group uses for log resale and bot affiliate program access, tools the group uses to monetize its activities, how the group accomplishes operational security, and how the group carried out its daily tasks. GTIC has released a whitepaper documenting the findings and analyzing the threat actor's working environment, which is available here.

Wizard Spider is one of the most nefarious cybercriminal groups currently in operation. The group maintains a high tempo of operations, including targeted ransomware campaigns via Grim Spider against high-value targets. The group's first known ransomware attack occurred in August 2018. Since that time, it has launched ransomware campaigns against targets ranging from hospitals to financial institutions.

Similarly, we delved into the operations of the threat actor Winnti Group, which our analysts track as Entity-1 (ENT-1). ENT-1 is highly active and runs multiple parallel operations, primarily targeting entities in Asia. In a recently published whitepaper, our analysts tracked ENT-1 operations from December 2020 to April 2021. By conducting traffic analysis of ENT-1's infrastructure during this time frame, we determined the group's periods of activity imply it is a fully-funded APT group; the group's periods of activity correspond strongly to routine working hours.

We found ENT-1's daily activities included exploiting GlassFish Server software versions 3.1.2 and below. After exploitation, ENT-1 deployed the Acunitex web vulnerability scanner, Cobalt Strike, and other toolsets, like Shadowpad, Spyder, and the Winnti backdoor. Overall, we observed ENT-1 conducting web vulnerability scanning against the media organizations in Hong Kong, Taiwan, and Japan; travel and transportation organizations in Hong Kong; government organizations in Australia, Mongolia, Myanmar, Vietnam, Japan, and Macao; and universities and telecom operators in Bahrain and Kuwait.

Further analysis by us found ENT-1 is constantly expanding and diversifying its toolset while also growing its network infrastructure. Such an evolution would be consistent with ENT-1's past activity. Researchers first discovered the group targeting the gaming industry in 2010. In the years since the group expanded its targeting scope, our research shows the group is continuing to evolve to support its operations.

To read more about Grim Spider, GTIC's analysis of the threat actor's environment, and recommendations concerning the group, please read the whitepaper here. For more information about ENT-1, including indicators of compromise and how we can help, please read the whitepaper here.

Quick look at the CTA Summer Olympics

Threat Assessment report

Lead Analyst: Jeannette Dickens-Hale, Senior All-Source Threat Intelligence Analyst, Global Threat Intelligence Center, US

The 2020 Olympics will take place this year in Tokyo, Japan, from 23 July to 08 August. As the Games approach opening ceremonies, the threat landscape increases and becomes more of a target for cyberthreat actors. In April 2021, the Cyber Threat Alliance (CTA) released an updated Summer Olympics Threat Assessment report. According to the report, the top three types of attacks most likely to occur are nation-state cyberattacks, ransomware attacks, disruptive and disinformation attacks.

Nation-state actors will pose the greatest threat to the Olympics and Olympics-affiliated entities. Russian, North Korean, and Chinese state-sponsored threat actors will most likely pose significant threats to the Olympic games based on geopolitical tensions and previous attack history. Although Iran is known to launch nation-state cyberattacks, an Iranian state-sponsored attack against the Olympic games and its affiliates would yield little strategic value for Iran.

Attacks will most likely occur before, during, and after the Games. Such attacks will most likely target national or international Olympic institutions that collect and process confidential athlete physical and medical information. If any exfiltrated data is released before or during the Games, it could cause maximum damage. Russian state-sponsored threat actors set a precedent for this type of retaliation when they launched a targeted attack against the World Anti-Doping Agency (WADA) in 2015-2016 and released athletes' personal and medical information.

The Olympic Games' high visibility and global reach make it an attractive target for ransomware attacks, including attacks against vendors or other organizations in the supply chain. Cybercriminals are likely to use this opportunity to launch disruptive attacks and disinformation campaigns. Distributed Denial of Service (DDoS) attacks, ransomware attacks, or attacks against critical infrastructure are most likely.

At high risk of compromise are anti-doping agencies and their key individuals, along with services supporting the Games' operations and logistics, such as Wi-Fi networks and ticketing systems. Other potential targets include tourists and spectators, Japanese officials, dignitaries from partner governments, Olympic partners and sponsors, and supply chain and infrastructure providers.

Geopolitical factors impacting the Games' security could include the belief that Japan has a weakened cybersecurity posture resulting from its domestic and regional issues and the COVID-19 pandemic, which could embolden threat actors to launch cyberattacks against Japan and the Games. Media reports that Japanese government officials were considering canceling the Games, the resignation of former Prime Minister Shinzo Abe, and perceived low Japanese support for the Olympics are a few domestic issues that could impact Japan's cybersecurity posture.

To defend against these cyberthreats, we support the CTA recommendations focusing on good cyber hygiene, ensuring that cybersecurity stakeholders follow best practices. In addition, regular information sharing between key stakeholders is essential to ensure that all parties establish active information flows.

Creating a coordinated cybersecurity plan before the Games will allow for early planning and allocation of necessary resources, including personnel and equipment. We agree with CTA recommendations that start with an in-depth risk assessment of potential threats and vulnerabilities before the Games commence to allow the organizers, cybersecurity providers, and stakeholders to make recommendations and establish action plans. Including a cybersecurity capabilities matrix that maps potential threats is an excellent addition to any mitigation solution.

NTT's Global Threat Intelligence Center

The NTT 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 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'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

2021 Global Threat Intelligence Report

Our 2021 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.


NTT