OTORIO

INDUSTRIAL CYBERCRIME IMPACT

REPORT

OT Security Strategic Predictions **2021**

Table of Contents

2020: The Rise of Cybercrime Against Industrial Operations

Executive Summary

2020 has been a remarkable year for cybersecurity in general and specifically for industrial cybersecurity. Not surprisingly, the memorable year was dominated by COVID-19. Forced lockdowns, travel bans, social distancing and a general fear of the pandemic have slowed the global economy almost to a halt. However, for the industrial sector and its just-in-time supply chain, COVID-19 actually served to accelerate processes such as remote access and remote management and operations. To maintain productivity and competitiveness, organizations were forced to open their production floor and allow remote access to both employees and vendors. Yet this rapid adoption of connectivity tools has become at times a double-edged sword – especially when proper digital and cybersecurity measures are lacking. And as with any gap in cybersecurity, hackers were quick to locate it, and exploit it.

Notable Trends in 2020:

Cyber criminals have identified industrial organizations as ill prepared and very lucrative. As a result:

1. Ransomware is on the rise - both as regards to the number of incidents targeting industrial companies and the impact of such attacks on production continuity.
2. Direct attacks against fragmented internet-exposed ICS are on the rise.
3. APTs are targeting supervisory systems rather than low-level OT.
4. APTs choose to adopt low-skill Tactics, Techniques and Procedures (TTPs), prioritizing functional and psychological impact over stealth.
5. As the need for remote working increases as a result of COVID-19, remote access systems become an increasing risk for operational resiliency.

The Industrial Sector Was Not Prepared for COVID-19 Effects

For over a decade, organizations across the globe and across all sectors are digitizing in order to improve efficiencies, increase yield and profit. This trend, also referred to as Industry 4.0, started long before COVID-19. Current events have given digitization efforts a significant boost.

Overwhelmed by the first wave of COVID-19 and its effects, manufacturers realized that they must become much more agile and resilient to disruptions in both production and supply chain management. Remote operations were accelerated in an attempt to cope with social distancing and travel restrictions. Employees were requested to work from home when possible while vendors and suppliers had to limit on-site visits for maintenance and support.

This has led to two conflicting trends. On the one hand, a rapid opening of production facilities to external users via the internet in an attempt to improve productivity, and on the other, an expansion of the organization's attack surface to a point where revenue-generating operations are at risk.

By enabling supply chain providers to support inner processes and systems, organizations place the security of their most valuable assets in the hands of their vendors. Thus, they expose their production floor to cyberattacks that can originate deep in their supply chain.

The industrial sector - which until recently was almost entirely air-gapped – was identified by cyber criminals as vulnerable, and is constantly (and often successfully) targeted. Unlike IT-centric enterprise environments, OT-centric industrial environments comprise multi-generation, multi-vendor and sometimes inherently insecure technology. This makes the offensive process - whether direct or through the supply chain – much easier than defensive operations. Trying to protect the OT network with tools designed for IT, which rely heavily on post-breach detection, can lead to serious risk exposures – as we will discuss further in this report.

Cybercrime - Ransomware is on the Rise, Competitive Tech Espionage Continues

During 2020, OTORIO collected information about 146 successful ransomware attacks against industrial companies, 75% of which were attributed to four large and sophisticated variants: Maze, Sodinokibi/REvil, NetWalker and Conti/Ryuk.

Companies from all sectors were targeted – those that were hit harder by the economic slowdown, such as the manufacturing, automotive, the transportation and the steel industries; as well as those who fared well during the crisis such as healthcare, shipping, pharmaceuticals, food and beverage, and energy providers. Several industrial companies were forced to halt their production due to ransomware attacks. Examples include:

Notable Ransomware Attacks - June-December 2020

June 2020, Honda confirmed that a Snake ransomware attack on the corporate network resulted in a temporary production line standstill

July 2020, Mattel - Leading US maker Mattel reported it was a victim of a ransomware attack that impacted their business operations

August 2020, Konica Minolta - Giant IT manufacturer's services and devices became unavailable due to a ransomware attack

September 2020, Eyewear giant Luxottica could not continue production in two of its plants for the same reason

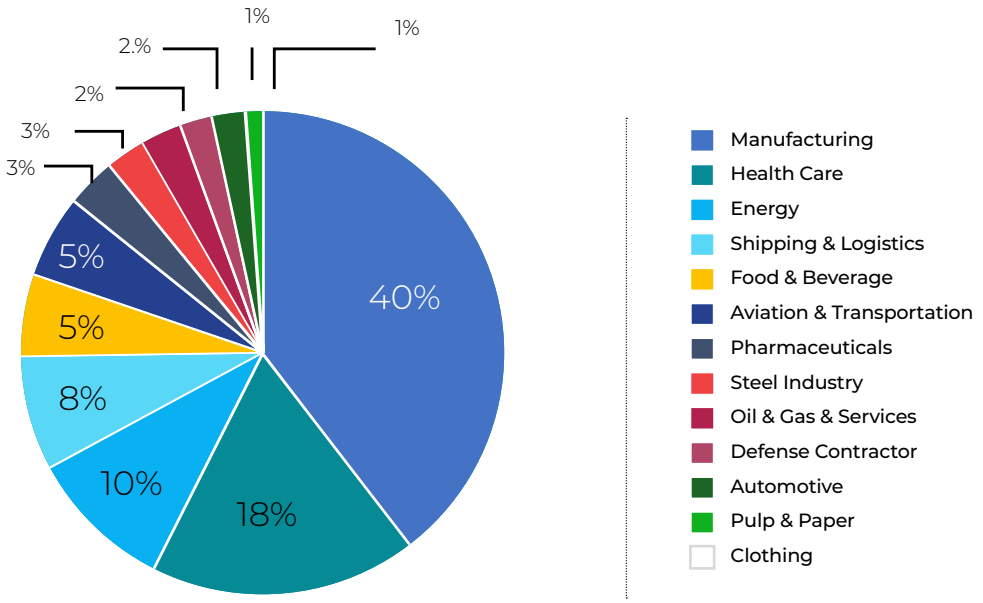
October 2020, Italian energy giant Enel was hit by Windows NetWalker ransomware

October 2020, A week after receiving approval to conduct phase 2/3 trials for COVID-19 vaccine, Dr Reddy's Laboratories had to shut down its manufacturing facilities around the world after they were hit by a cyber attack.

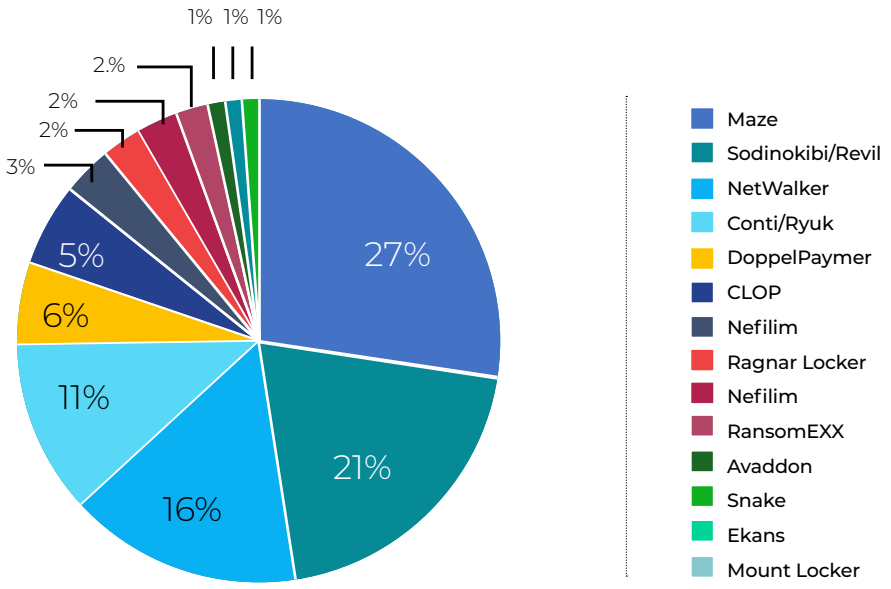
November 2020, IIoT chip maker Advantech was hit by ransomware and paid $12.5 million in ransom

Even when the impact is temporary – with no health hazards or long-term equipment damage - stopping the production of an industrial company causes tremendous pressure, arguably more than that caused to a law firm by a data leak. Moreover, damage to industrial companies has a clear physical scope – and results in loss of income due to replacement or repair of equipment damaged by the hack. As the majority of industrial-related hacks are originated by cyber criminals and not nation state actors, even when a ransomware attack does not reach the PLC itself, it significantly impacts industrial operations and comes at a cost.

Industrial Ransomware Attack Distribution by Industry



Source: OTORIO, Understanding the Ransomware Victim Profile [1]



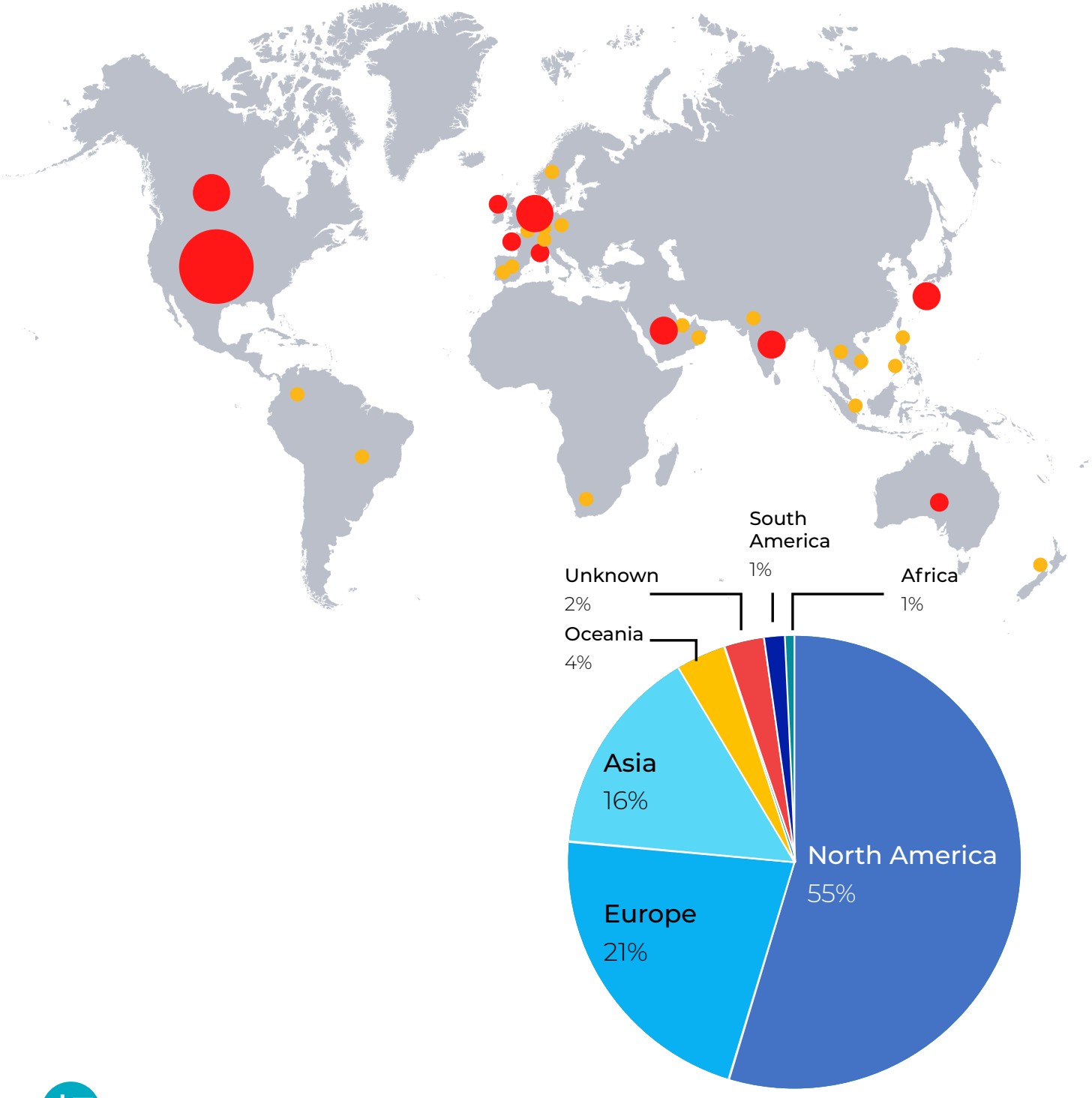
Source: OTORIO, Understanding the Ransomware Victim Profile

1 https://www.otorio.com/blog/understanding-the-ransomware-victim-profile-part-one/

COVID-19 Accelerated Ransomware Attacks Targeting Industrial Companies

An increase in Ransomware attacks was seen in companies from all sectors during 2020. Hackers took advantage of the fast shift to opening the shop floor to remote connections. As a result, we have seen a surge in industrial ransomware attacks from less than five successful attacks per month in the first quarter of the year, to over twenty successful attacks per month from May onwards. The geographical spread has left no populated continent safe. We've seen attacks in 31 countries located in Africa, Asia, Europe, Oceania, South America and North America. Almost 55% of attack victims were North America-based companies, more than 20% were European-based and more than 15% were Asia-based.

Industrial Attacks - Global Distribution



The Ransomware Victim Profile – Assess Your Risk

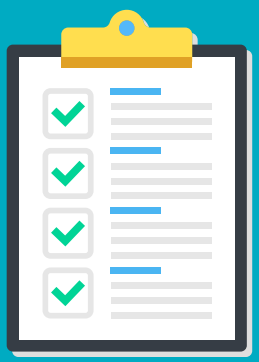
To understand the impact of ransomware attacks - and why they continue to wreak havoc on companies and entire industries - we first need to understand their violent nature. Aside from the significant financial and reputational damage they cause, ransomware attacks have an added effect of psychological pressure that resembles the randomness of terrorist acts - they can hit virtually anyone. Not surprisingly, ransomware threats are on the top of the list of concerns of CISOs and executives across numerous industries.

When large corporations such as Honda, ENEL, or PEMEX are attacked, they can't escape admitting it. And the pressure to "get their network back" is immense. As the level of anxiety and frustration on the victim's side soars, pressure from customers, suppliers and shareholders, not to mention the media and the competition, add fuel to the fire. This is exactly the situation the attacker desires, as the victim is more likely to agree to quickly pay the ransom.

In contrast to the above, little is reported about small, medium, and large industrial companies that suffer ransomware attacks. OTORIO's Incident Response team is often called upon to deal with ransomware attacks on industrial companies worldwide. Based on their experience, we can confirm that attacks on small and mid-sized companies are just as devastating and impactful as those that hit huge enterprises.

Ransomware can hit anyone unexpectedly, yet we see that some organizations are at higher risk. Therefore, the earlier a company understands its "victim profile," a term that represents the perception of a ransomware attacker, the better it can defend its assets and prepare employees, suppliers, clients, and internal stakeholders for a potential attack.

OTORIO researchers and risk assessment teams work with clients to help them understand and score the chance of being hit by ransomware, and prepare accordingly. In the process, they have developed a short series of questions that help companies understand their "victim profile." If the majority of the answers are "yes", then the "victim score" is high and the company should start taking preemptive steps:



Understand Your Ransomware Victim Profile

- ☑ Is your business vertical in the headlines?
- ☑ Are you a supplier of critical materials, products, or services?
- ☑ Do you supply anything that is delay- or shortage-sensitive?
- ☑ Are you a supplier for governments, defense, or advanced technologies?
- ☑ Do you or your partners own unique intellectual property?
- ☑ Do you depend on your IT/OT network for business continuity?
- ☑ Does your company retain client and/or employee PII?

For more on this visit our blog page or listen to our Victim Profile Webinar.

“Traditional” Data Theft is Still in Style

Although today’s ransomware attacks make up a large portion of the known cyberattacks against industries, we still notice “classical” cyberattacks that intend to steal information in order to eliminate competitive advantages and/or damage reputation. Among such attacks was the attempt to propagate crafter malware in the network of one of Tesla’s factories in August 2020[2], and massive leaks of technical information and patent documents from other automotive manufacturers.

Recently, attacks on healthcare facilities and pharmaceutical companies - all under tremendous pressure to deal with COVID - have increased in number and intensity. Notable attacks include those on India’s Dr. Reddy’s Laboratories in October and Lupin Laboratories in November.

APTs - Persistent, High-Skill Attacks

An especially interesting campaign in 2020 is PoetRAT[3], which was first detected in February 2020 . The phishing campaign used government-masqueraded Word documents, which later dropped a dynamic data stealer. The victims of this campaign were mostly energy companies and organizations in Azerbaijan. Judging by the propagation of the tool and its activity, it was clearly focused on SCADA systems, such as those that manage wind turbines. OTORIO’s researchers concluded that the attackers’ choice to focus on supervisory systems reflect offensive intentions that include loss of visibility through injection of fictitious data, to forced shutdown.

APTs - Low - Skill Attacks Involving Immediate Access to ICS

Low skill attacks probably pose the greatest threat to industrial systems. There is a steep cliff between the high impact of such an attack on public health, safety, and mindset - and the rather low level of sophistication needed to carry out the attack.

One example was the attempt to infiltrate several Israeli Water Authority sites in April 2020. According to official announcements, the hackers managed to gain access to several controllers after searching for exposed assets on Shodan, a search engine dedicated to finding computers, servers, machines, and devices connected to the internet.

With more ICS components connecting every day to the internet (over 125,000 if we count only direct connection through industrial ports and protocols[4]), attackers have a wide choice of targets that often have a direct impact on safety and human lives.

Understanding the huge potential damage, OTORIO integrated scans for exposed ICSs in its automated reconnaissance, and reported several cases of ICS exposure where an attack would have led to devastating results.

2 *https://www.wired.com/story/tesla-ransomware-insider-hack-attempt/*
3 *https://blog.talosintelligence.com/2020/04/poetrat-COVID-19-lures.html*
4 *https://blog.shodan.io/trends-in-internet-exposure/*

The Rising Risk of Remote Connectivity

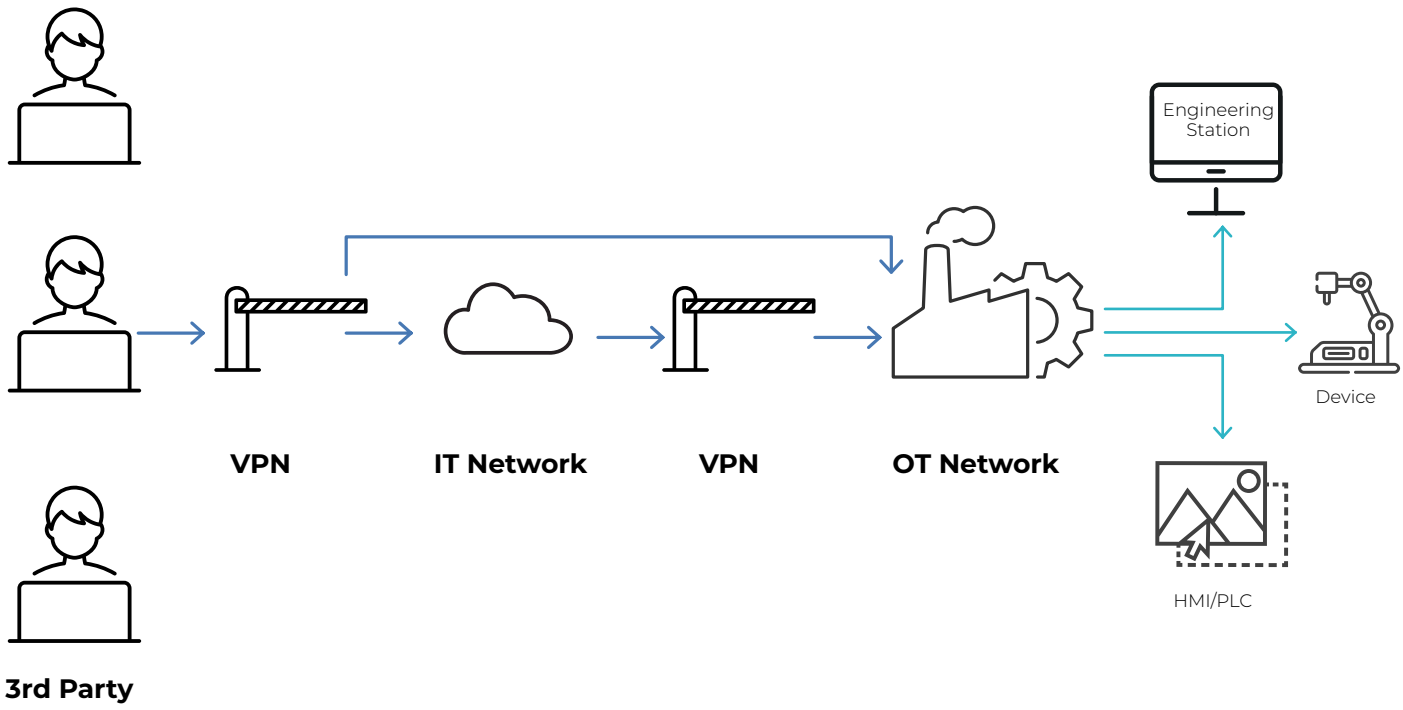
Much has been discussed about the changes that COVID-19 precipitated. But perhaps one of its most significant impacts on the industrial sector is that it pushed manufacturers to rely heavily on remote access to OT networks.

Remote access solutions that were already in use prior to COVID-19 were adopted at an accelerated pace. At the same time, organizations that until recently refrained from connecting their production floor to the Internet were forced to do so in order to keep production and operations running. Furthermore, we continue to see a lot of basic VPN connections used by suppliers, without sufficient hardening. These legacy VPN solutions create gaps in remote access security and are a virtual 'ticking bomb', waiting to detonate.

Although we have yet to see a major attack that utilizes industrial remote connection access solutions, we do see a rise in the exposure of such systems and in the attempts to scan them. In the OT world, standards and norms of awareness lag behind those in the IT domain. The OT world still lacks proper prevention and detection mechanisms as well as trusted synchronization between defenders, researchers and regulators.

Going forward, next generation remote access systems need to provide a single-point-of-entry to the production floor and its assets. These systems need to allow admins to manage user access permissions at both the asset level and the connection protocol level, while logging every access or action to ensure full visibility, with a clear audit trail and effective vendor governance.

Over the past months, OTORIO's researchers have discovered a number of vulnerabilities in remote access systems. These vulnerabilities have one thing in common: they are easily exploitable and when exploited, can cause a lot of damage.



Analysis of the Adversarial Landscape

When discussing the different potential adversaries an industrial business might face, OTORIO prefers to divide the threat actors roughly into two groups, representing their goals, techniques and tactics, alongside their offensive goal. The fact that only very few "pure OT" attacks have been ever published, makes it even more important to try to conceptualize the adversarial landscape, as seen in the chart below, in order to develop and implement adequate security measures.

Attacker Type	Attacker Nationality	Goals	Techniques	Notable Tactics	Impact
Nation state backed groups (Financial)	China, North Korea, Vietnam, Russia, Iran	Competitive espionage, technological advantage	Clandestine, persistent, wide network attacks	Supply chain attacks, attacks on third parties	Theft of intellectual property and business secrets
Nation state backed groups (Political)		Psychological warfare, damage to sensitive facilities and processes		Supply chain attacks, insider threat	Cutting off or disrupting critical processes and infrastructures
Cyber-Criminals	International	Financial profit through ransom blackmail	Network attacks to steal data or impact production, ransomware to claim money	Phishing, increased use of remote connection solutions (RDP, Citrix)	Production slowdown / halt, business disruption, loss of reputation

Vulnerabilities and Exploits

Over the first nine months of 2020, 322 new vulnerabilities were disclosed and reported in industrial automation and control systems. This number already exceeds the 2019 annual "vulnerability yield".

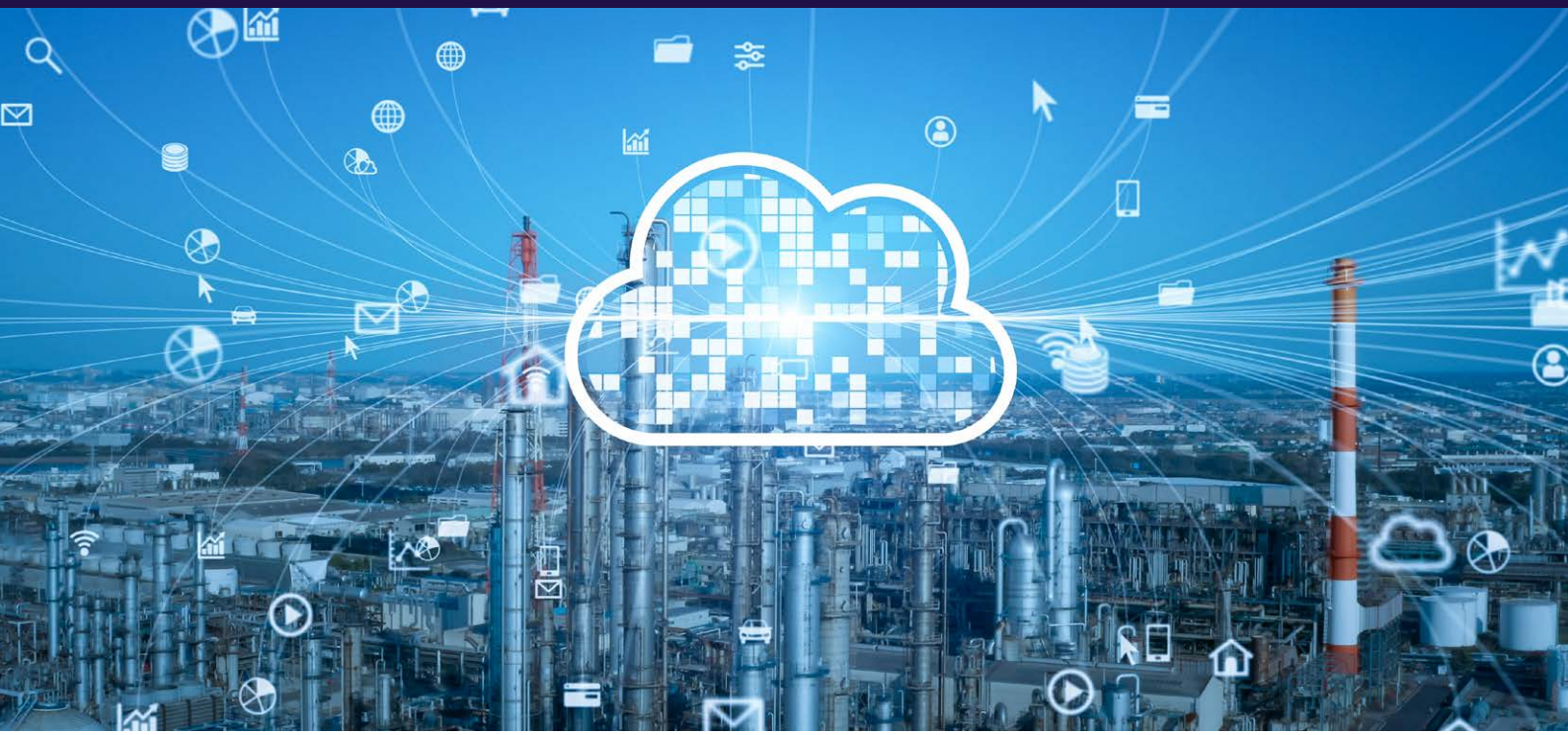
As in the past few years, most of the vulnerabilities were discovered in products from industrial giants such as Siemens, Schneider Electric, ABB, Moxa, Mitsubishi and others. The interesting trend, however, is that there is a rise in the number of vulnerabilities in automation software, supervisory and remote access solutions.

Vulnerability research is partially biased, as researchers "play" with what they have at hand or, in many cases, with what they consider to be important and critical. Therefore, we should not conclude that remote access solutions, for instance, have become more vulnerable in 2020. Rather, they are now under the lens of the researchers' microscopes because their impact on business continuity has increased significantly. As mentioned above, OTORIO's research focused this year on classic **low level vulnerabilities**, which are highly applicable to multiple products, along with vulnerabilities in **historians** and **remote access solutions.**

Over the first nine months of 2020

322

new OT vulnerabilities



Assessments and Predictions for 2021

Predictions are always hard to make, and doing so for 2021 – especially given the imminent COVID-19 vaccine and its influence on the global economy - is even harder. Yet based on our deep domain knowledge and years of hands-on experience, OTORIO expects that in 2021:

01 Ransomware will physically impact production.

2021 will see a substantial increase in the number of companies affected by ransomware. Rather than settling for data theft, cybercriminals are increasing their attempts to disrupt production by praying on production floors and backup systems. This in turn leads to revenue loss and potentially substantial production recovery costs. The rate of new variant appearance also continues to grow while the existing strains focus on "expanding business". As a result, executive teams (as well as industry insurers) will take a more active role in both preparing for attacks in order to minimizing losses, as well as taking proactive risk avoidance measures.

02 Remote access to industrial production floors will be a primary risk.

Travel restrictions and social distancing will continue to be observed in 2021, leading more organizations to rely on remote access connectivity. This growing dependency on remote access solutions makes them a primary target for cybercriminals as they provide a "highway to OT" that replaces the good old kill chain[5] . Industrial organizations will do well to demand of their system vendors and service providers to comply with strict cybersecurity regulations and to shorten response time between discovery of vulnerabilities and mitigating them. At the same time, remote accesses system providers must invest more in testing the security of their products, and do so continuously. Finally, industrial cybersecurity professionals will have to build automation and governance processes to maintain version updates and patches and bring the security standards of industrial remote access to be on par with those of IT teleworking.

5 https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

03 Attacks on OT will become more significant throughout geopolitical tensions.

This means that the "time to market" of such attacks will be shortened. Owners of critical infrastructures will have to beef up their security stack not only with more intelligence and detection, but also with playbooks, penetration tests and incident response drills.

04 C-level management will become more involved in OT cybersecurity.

Ransomware is transforming from being a nuisance to becoming a real threat to the organization's production capabilities. The focus of executive managements shifts towards OT security, as do responsibilities. We expect to see more CIOs, CISOs sometimes even CEOs taking responsibility over OT network security in 2021 and beyond. This trend will accelerate as regulation and compliance demands increasingly focus on C-suite liability and responsibility in case of damages caused by cyber attacks.

05 To cope with reduced budgets, CSOs and CISOs will seek convergence across security solutions.

Seeking unified digital and cybersecurity operations - for both IT and OT - makes perfect sense from a pure security governance and control perspective. Yet until today, IT and OT convergence were moving at a slow pace. The growing number of attacks on OT networks, along with the financial pressures caused by COVID-19, are now accelerating this process.

06 Commonly used threat detection paradigms will be replaced by proactive risk avoidance approaches.

With the need to provide governance in times of uncertainty, organizations will look for new approaches to OT security. Intruder and anomaly detection tools may be good to flag out cyber incidents in progress – but industrial organizations who need to secure their revenue generating operations, are starting to apply predictive risk avoidance approaches in order to map gaps in their security posture long before they turn into breaches.

About OTORIO

OTORIO designs and markets the next generation of OT security and digital risk management solutions. The company combines the experience of top nation-state cybersecurity experts with cutting edge digital risk management technologies to provide the highest level of protection for the manufacturing industry. Visit our website: www.otorio.com

Appendix A – Making the World a Safer Place

Vulnerabilities discovered and filed by OTORIO researchers in 2020

Name	CVE Number	Software/ Hardware	Industries	Vulnerability Explained
PI Web API 2019 Vulnerability	CVE-2020-12021/ ICSA-20-163-01	OSIsoft PI Server	Variety	PI Web API 2019 component of PI System is affected by a stored XSS vulnerability that allows an attacker with limited privileges on the targeted system to conduct various types of activities
Siemens	CVE-2019-13946	Numerous Siemens	Variety	Inside the implementation of the Profinet(R) stack in Siemens devices including distributed I/Os (SIMATIC ET200), communication modules (SIMATIC CP) and industrial switches (SCALANCE). These devices are used among other things, to connect dispersed IoT devices with core systems, networks and processes and serve critical infrastructure in verticals ranging from power generation and distribution, Oil & Gas, Transportation, and more. Failing to patch the vulnerability could have hazardous consequences including power outages, failure of traffic control systems, disrupted operations and more.
Moxa	CVE-2019-19707	Moxa's EDS-G508E, EDS-G512E, and EDS-G516E Series Ethernet Switches.	Variety	Denial of service by PROFINET DCE-RPC endpoint discovery packets (CWE-400). To exploit this vulnerability, the attacker may cause the target device to go out of service.
SIEMENS X-200 OT Switches	CVE-2013-3633	SIEMENS X-200 OT Switches	SCADA / OT	The user privileges for the web interface are only enforced on client side and not properly verified on server side. Therefore, an attacker is able to execute privileged commands using an unprivileged account.
MB Connect line mbCONNECT24	CVE-2020-24568 - Blind SQL injection on mbConnect service	MB Connect line	SCADA / OT	Successful exploitation of these vulnerabilities could allow a remote attacker to gain unauthorized access to arbitrary information or allow remote code execution.
MB Connect line mbCONNECT24	CVE-2020-24569 - Blind SQL injection on mbConnect	MB Connect line	SCADA / OT	Successful exploitation of these vulnerabilities could allow a remote attacker to gain unauthorized access to arbitrary information or allow remote code execution.

Name	CVE Number	Software/ Hardware	Industries	Vulnerability Explained
MB Connect line mbCONNECT24	CVE-2020-24570 - SSRF/CSRF on mbConnect service	MB Connect line	SCADA / OT	Successful exploitation of these vulnerabilities could allow a remote attacker to gain unauthorized access to arbitrary information or allow remote code execution.
B&R GateManager and SiteManager	CVE-2020-11641 - SiteManager Local File Inclusion Vulnerability	B&R GateManager and SiteManager	SCADA / OT	Successful exploitation of these vulnerabilities could allow for arbitrary information disclosure, manipulation, and a denial-of-service condition.
B&R GateManager and SiteManager	CVE-2020-11642 - SiteManager Denial of Service via Local File Inclusion Vulnerability	B&R GateManager and SiteManager	SCADA / OT	Successful exploitation of these vulnerabilities could allow for arbitrary information disclosure, manipulation, and a denial-of-service condition.
B&R GateManager and SiteManager	CVE-2020-11643 - GateManager Information Disclosure Vulnerability	B&R GateManager and SiteManager	SCADA / OT	Successful exploitation of these vulnerabilities could allow for arbitrary information disclosure, manipulation, and a denial-of-service condition.
B&R GateManager and SiteManager	CVE-2020-11644 - GateManager Audit Message Spoofing Vulnerability	B&R GateManager and SiteManager	SCADA / OT	Successful exploitation of these vulnerabilities could allow for arbitrary information disclosure, manipulation, and a denial-of-service condition.
B&R GateManager and SiteManager	CVE-2020-11645 - GateManager Denial of Service Vulnerability	B&R GateManager and SiteManager	SCADA / OT	Successful exploitation of these vulnerabilities could allow for arbitrary information disclosure, manipulation, and a denial-of-service condition.
B&R GateManager and SiteManager	CVE-2020-11646 - GateManager Log Information Disclosure Vulnerability	B&R GateManager and SiteManager	SCADA / OT	Successful exploitation of these vulnerabilities could allow for arbitrary information disclosure, manipulation, and a denial-of-service condition.
Siemens PCS 7	Configuration issue	Siemens PCS 7	SCADA / OT	The default PCS 7 setup process creates three default user groups. One of the user groups, the Simatic HMI, has access to execute runtime executables. By default, the user in the installation is added to the Simatic HMI group even if s/he is in the administration group.
Siemens PCS 7	Configuration issue	Siemens PCS 7	SCADA / OT	WinCC is a PCS 7 component. When an engineer downloads a WinCC project from the engineering station to the OS stations, s/he specifies a network drive - a shared folder - on the OS station. The project is then saved on the shared folder. It is safe to believe that without clear instructions, a user installing PCS 7 may set access to the shared folder as set to "Everyone" with "Full Control".

Appendix B

Testing Security Mechanisms with Real-life IT/OT Scenarios

OT environments are almost always unique, therefore, creating a testbed for them requires customization which is not always available when using off-the-shelf solutions like those available on the market today. In June 2020, OTORIO researchers presented a tool that allows organizations to test their security systems in a real-life ICS environment.

When designing a testbed for a network, it is important to define the techniques and attack scenarios that are most relevant to your line of business. Relying only on past experience or known TTPs will leave the network vulnerable, as defenses will always be several steps behind the attacker. To overcome this limitation, OTORIO's Research Team has created 24 test scenarios dedicated to OT.

The OTORIO solution uses Caldera, an open source tool, and leverages MITRE ATT&CK[6] in Caldera, to facilitate the process of choosing attack abilities and scenario creation. The user chooses the desired ability, which is a specific implementation of a technique that is a part of ATT&CK's tactics.

IMPORTANT NOTE: Because of the sensitivity of creating attack tools, OT Caldera is not open sourced. However, researchers from the ICS community are encouraged to reach out to our team for additional information and knowledge sharing.

The attack scenarios are listed below. The full white paper can be downloaded from OTORIO's Resource Center.

Attack Scenarios

1. COLLECTION | DATA FROM INFORMATION REPOSITORIES | Find Cimplicity files by extensions
2. COLLECTION | DATA FROM INFORMATION REPOSITORIES | Find industrial files by extensions
3. COLLECTION | POINT & TAG IDENTIFICATION | Query OPC tags
4. COLLECTION | PROGRAM UPLOAD | Upload Schneider PLC code
5. COMMAND-AND-CONTROL | ENCRYPTED CHANNEL | Cimplicty Secure Communications Check
6. DISCOVERY | CONTROL DEVICE IDENTIFICATION | BACnet scan
7. DISCOVERY | CONTROL DEVICE IDENTIFICATION | DCE/RPC scan
8. DISCOVERY | CONTROL DEVICE IDENTIFICATION | DNP3 scan
9. DISCOVERY | CONTROL DEVICE IDENTIFICATION | Ethernet/IP scan
10. 1DISCOVERY | CONTROL DEVICE IDENTIFICATION | IEC 104 scan
11. DISCOVERY | CONTROL DEVICE IDENTIFICATION | Modbus scan
12. DISCOVERY | CONTROL DEVICE IDENTIFICATION | OPC API query
13. DISCOVERY | CONTROL DEVICE IDENTIFICATION | Query IEC 61850 values
14. DISCOVERY | CONTROL DEVICE IDENTIFICATION | S7 scan
15. DISCOVERY | I/O MODULE DISCOVERY | Query Modbus coils
16. DISCOVERY | NETWORK SERVICE SCANNING | Industrial port scan
17. DISCOVERY | PERMISSION GROUPS DISCOVERY | Cimplicity Installation Folder Permission Discovery
18. IMPACT | MANIPULATION OF CONTROL | IP Change via DCP
19. IMPAIR-PROCESS-CONTROL | BRUTE FORCE I/O | Brute Force Modbus coils
20. INHIBIT-RESPONSE-FUNCTION | DENIAL OF SERVICE | Sockstress DoS
21. INHIBIT-RESPONSE-FUNCTION | DEVICE RESTART/SHUTDOWN | Start PLC s7 command
22. INHIBIT-RESPONSE-FUNCTION | DEVICE RESTART/SHUTDOWN | Stop PLC s7 command
23. LATERAL-MOVEMENT | DEFAULT CREDENTIALS | Discover ScalanceX default http credentials
24. LATERAL-MOVEMENT | DEFAULT CREDENTIALS | Discover ScalanceX default telnet credentials

---

6 ATT&CK was designed with IT networks in mind. ATT&CK for Industrial Control Systems (ICS) is the OT version of MITRE ATT&CK. It introduces many new abilities, such as project file injection, ladder logic modification, and more. ATT&CK for ICS is a good starting point to assemble all known techniques, tactics, and procedures (TTPs).

