OTORIO

INDUSTRIAL CYBERCRIME IMPACT

Q1 2021 REPORT

Table of Contents

2021: Cyberattacks Physically Impact Operations

More than a year after the World Health Organization declared the Covid-19 outbreak a pandemic, and the crisis is far from over. The manufacturing and critical infrastructures industries were dramatically impacted by the pandemic – including operational disruptions, productivity loss and lower sales. As a result, most companies had to reevaluate their operating models and increase the use of digital enablers like automation, remote access solutions, IT-OT convergence, and cloud technologies.

Unfortunately, 2020 broke records when it came to sheer numbers of cyberattacks on industrial and critical infrastructure organizations, as well as on governments and individuals.

As OTORIO sadly predicted in our 2020 Industrial Cybercrime Impact Report, the challenges stemming from increased remote operations, alongside heightened hacker awareness of the inherent vulnerabilities of OT networks, have led to a steep rise in cyberattacks on industrial and critical infrastructure targets in the first quarter of 2021.

In this report update, we discuss the top trends of 2021: dramatic rise in disruptive industrial cyberattacks, ransomware, remote access vulnerabilities exploits and phishing attacks. We then review notable attacks in the most impacted sectors: water treatments, utilities, maritime, automotive and healthcare. We will then discuss the impact of the 2021 cyberattacks on production and operations. Finally, we will review recent remote access and VPN vulnerabilities.

01. Notable Trends in 2021

1.1. Disruptive Industrial Cyber Attacks Have Doubled in Q1/2021

Since January, we've seen a dramatic rise in the number of attacks that have affected the operations of large manufacturing plants and critical infrastructure sites. Utilities such as water treatment plants, fuel distributors, energy utilities and hospitals are getting a concerning amount of attention from hackers.

In Q1 of 2021, the operations of 14 industrial companies and critical infrastructure sites were disrupted by cyberattacks - more cases than in Q3 and Q4 2020 together, and a 200% increase compared to Q4 2020.

Further to the 2020 rise of cyberattacks targeting industrial companies, in Q1 2021 we're seeing that as attackers get more experienced, they manage to cause more severe damage. This probably explains why the new US administration is taking this operational cybersecurity threat very seriously and is expected to soon issue an executive order focused on industrial control systems that operate utilities such as water treatment and energy delivery.

Industrial cyberattacks that disrupted operations in 2020-2021

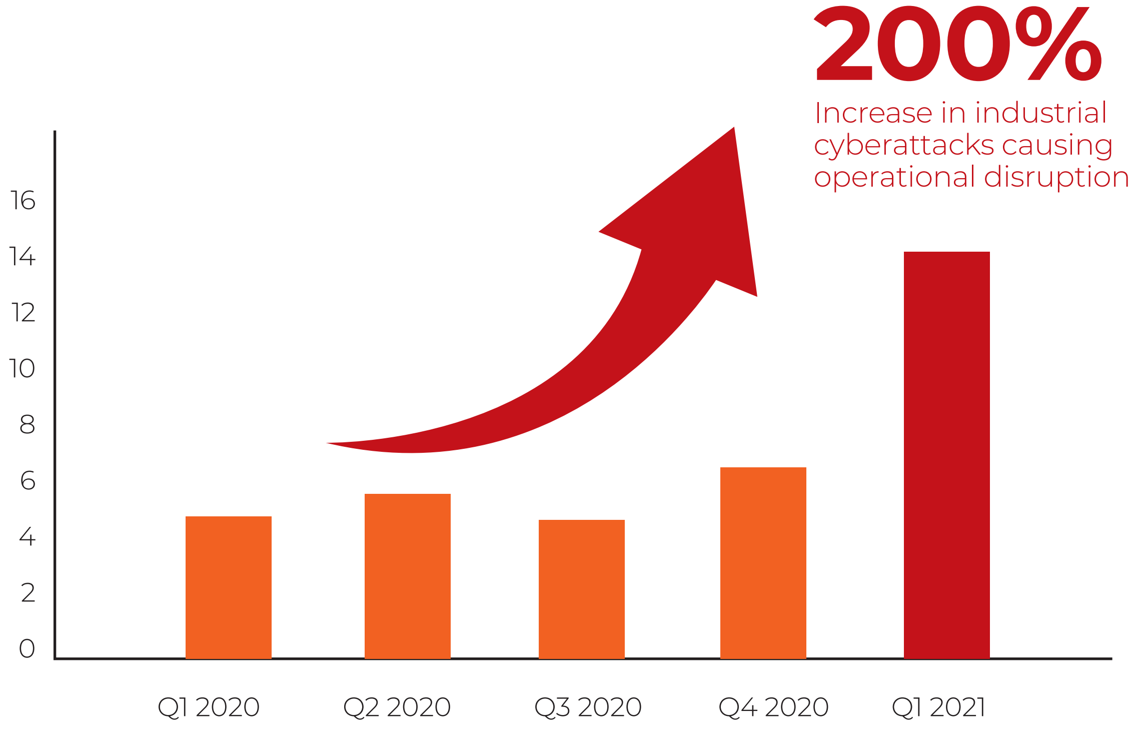


Diagram 1: 2020-2021 Industrial cyberattacks that disrupted operations

1.2. Ransomware: A Growing Threat

In Q1 2021, the industrial sector at large is increasingly in the crosshairs of ransomware threat actors. At least 70% of the major attacks that targeted operational networks in the first quarter of this year were ransomware attacks.[1]

Types of attacks on industrial networks

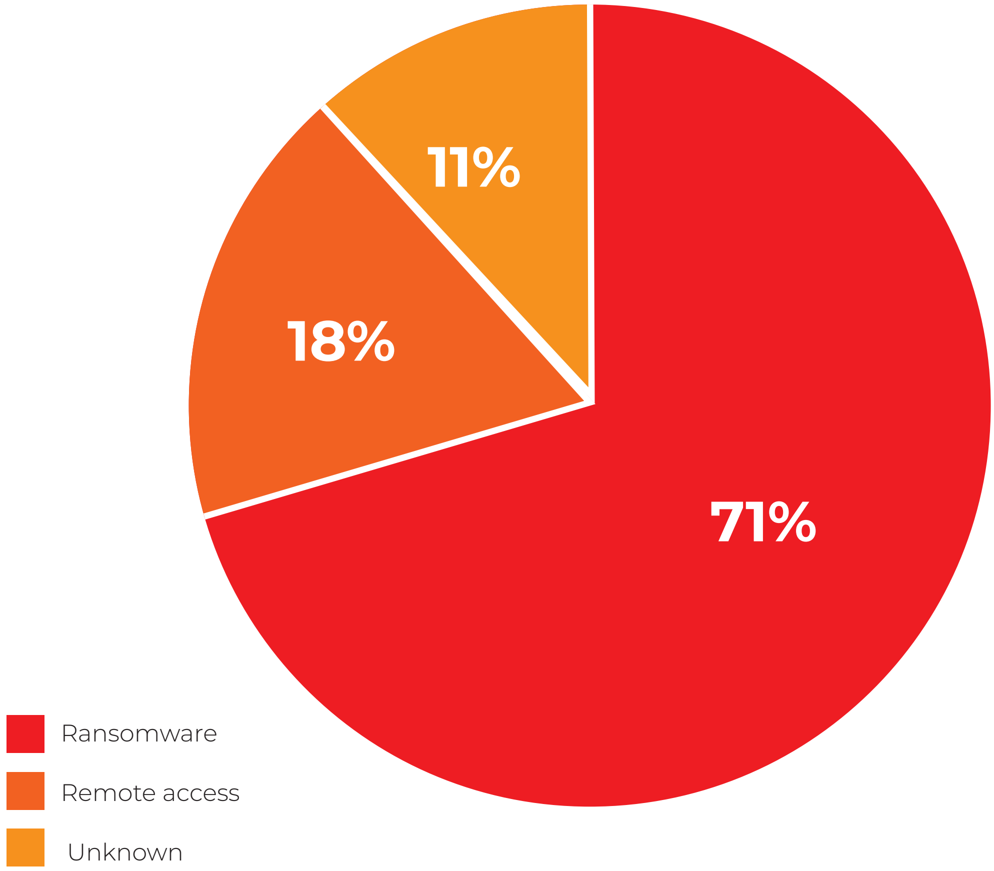


Diagram 2: Q1/21 types of attacks on industrial networks

[1] OTORIO research, Temple University - Rege, A. (2021). "Critical Infrastructure Ransomware Incident Dataset". Version 10.9. Temple University. Online at https://sites.temple.edu/care/resources/. Funded by National Science Foundation CAREER Award #1453040.

Ramsomware attacks across all sectors are growing bolder, more frequent, and exponentially more expensive. In fact, ransomware attacks targeting industry were second only to those targeting government in prevalence[2].

Ransomware threat actors are increasingly adopting more sophisticated techniques to threaten manufacturing operations and critical infrastructures. Notably, experts are tracking more frequent incorporation of code that seeks out and exploits vulnerabilities in industrial control systems (ICSs) and can spread from IT networks to OT networks.

Ransomware costs to the manufacturing sector have never been higher[3]. In 2019, industrial companies spent more than any others on ransomware payments – some $6.9M in payouts to hackers, which was 62% of the over $11M in ransomware payoffs in that year, despite the fact that manufacturing made up just 18% of ransomware cases. In 2020, that number rose even further, with the cross-industry cost of ransomware reaching some $20 billion[4].

However, ransomware payouts do not tell the whole story. Nor does paying off the attacker mean that the attack is over. In order to understand the real impact of this phenomenon, we need to look deeper. Recovery time from a cyberattack for industrial companies is 17 days on average, with some companies reporting weeks and even months before they are able to return to full production. Even if we use a modest estimate of $250K lost for every day of disruption, we are looking at costs in the millions.

Some of the most notable ransomware attacks that took place in the first three months of 2021 are:

- WestRock Co, the paper and packaging giant, was hit with a ransomware attack that caused severe disruption in the company's production and shipping capabilities, dropping the company's stock by 11% in only one week.
- Two French hospitals that were hit by the Ryuk ransomware at the same week were paralyzed by the attacks after refusing to pay the ransoms.
- The Cring Ransomware series of attacks against industrial targets and control systems (ICS) that exploited Fortinet's VPN server.

Recovery time from a cyberattack for industrial companies is **17 days on average**

[2] https://www.blackfog.com/the-state-of-ransomware-in-2020/

[3] https://www.infosecurity-magazine.com/news/manufacturing-ransomware-payments/

[4] https://purplesec.us/resources/cyber-security-statistics/ransomware/#:~:text=The%20estimated%20cost%20of%20ransomware,2018%20%E2%80%93%20%248%20billion

1.3. Remote Access Attacks – The Next Frontier

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.

Travel restrictions and social distancing continue to be observed in 2021. As a consequence, organizations continue to rely on remote access connectivity and plan to continue doing so in the coming years.

This growing dependency on remote access solutions makes them a primary target for cybercriminals. In 2020, 20% of organizations faced a security breach as a result of a remote worker[5]. This comes as no surprise, as attacks targeting remote access vulnerabilities increased by 768% between Q1 and Q4 2020[6].
This fact should concern industrial organizations as it provides attackers with a “highway to OT” that replaces the traditional kill chain.

As their importance to production and business continuity grows, remote access systems remain the Achilles heel of digitized industry in 2021.
Over the first quarter of 2021, more than 52 new vulnerabilities were disclosed and reported in industrial automation and control systems, most of them related to remote access.

Some of the most notable remote access attacks that took place in the first three months of 2021 are:

- The Florida Water Treatment was accessed remotely by a hacker who manipulated the water supply’s sodium hydroxide levels.
- The operations of at least two manufacturing plants were disrupted due to a FortiGate VPN vulnerability.

[5] https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf

[6] https://www.welivesecurity.com/2021/02/08/eset-threat-report-q42020/

1.4. Phishing Campaigns

Hackers and cyber scammers are taking advantage of the Covid-19 pandemic by sending fraudulent email and mobile messages with Covid-19 related information that tempt users into clicking on malicious links or opening attachments that contain malware. In the first few months of the pandemic, we saw an increase of almost 700% in phishing attacks, many containing pandemic-related keywords.

Now, in 2021, cybercriminals are trying to leverage vaccines to execute successful phishing campaigns. The FBI issued a warning in December about emerging fraud schemes related to Covid-19 vaccines[7].

Phishing campaigns are a huge risk to manufacturers and critical infrastructure utilities, especially as relates to remote work. With many employees operating the production floor and operational networks from afar, successful phishing attacks can give attackers direct access to the operational network.

Earlier this year, OTORIO researchers joined forces with Check Point Research[8] to analyze and take a deep dive into a large-scale phishing campaign that targeted thousands of global organizations, revealing the campaign's overall infection chain, infrastructure and how the emails were distributed. Attackers initiated a phishing campaign that successfully bypassed Microsoft Office 365 Advanced Threat Protection (ATP) filtering and stole over a thousand corporate employees' credentials. Interestingly, due to a simple mistake in their attack chain, the attackers behind the phishing campaign exposed the credentials they had stolen to the public Internet. With a simple Google search, anyone could have found the stolen credentials: a gift to every opportunistic attacker.

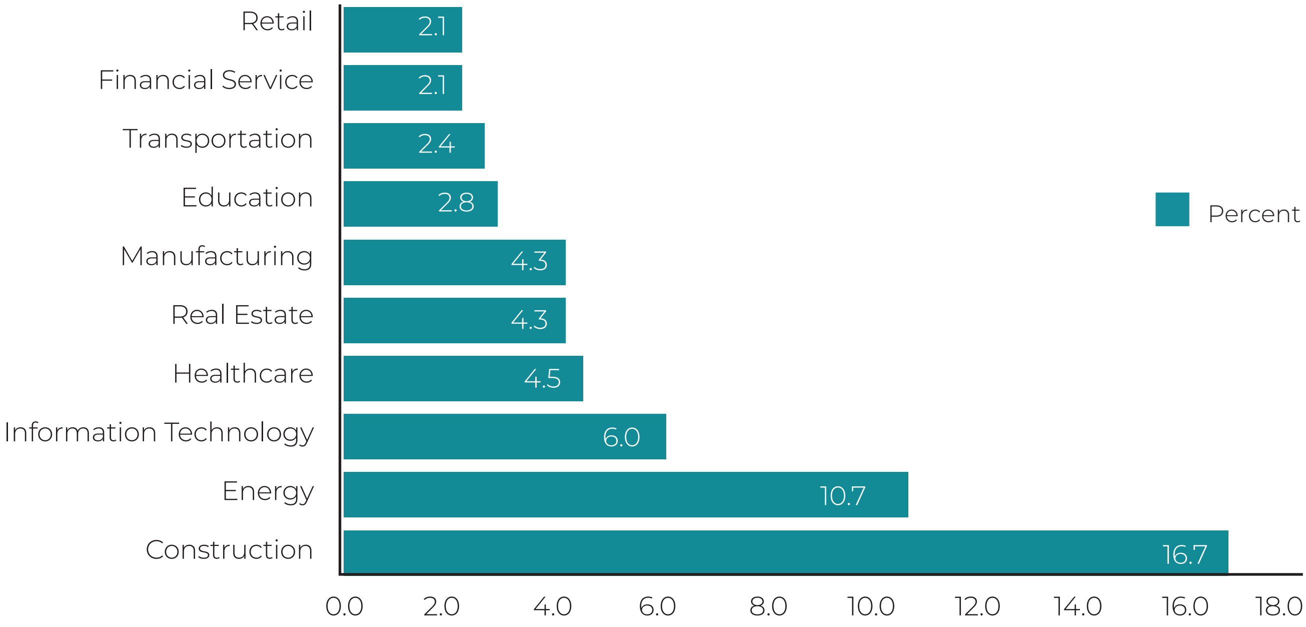


Diagram 3: Phishing Campaign Targets[8]

[7] https://www.mercurynews.com/2020/12/24/feds-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines/

[8] https://blog.checkpoint.com/2021/01/21/cyber-criminals-leave-stolen-phishing-credentials-in-plain-sight/

02. Target Industries

2.1. Water Utilities

Water treatment and distribution is mission-critical by any standards – providing the most basic and crucial of resources for businesses and homes. Yet treatment and distribution operations – frequently powered by legacy systems - remain highly exposed to cyberattacks.

In February 2021, hackers gained access to the water treatment system of Oldsmar, Florida[9], a town of nearly 14,000 residents. They manipulated the water supply's sodium hydroxide (lye) levels - which could have endangered thousands of lives had it not been detected so quickly by a resourceful employee.

The perpetrator gained access to the Oldsmar plant's systems via a poorly-protected version of TeamViewer, a tool in wide use to manage remote access to IT systems. The facility had actually stopped using TeamViewer six months prior to the attack, but had left it installed. The attack used stolen credentials that were shared between multiple users and devices to remotely login to the HMI station controlling the water systems.

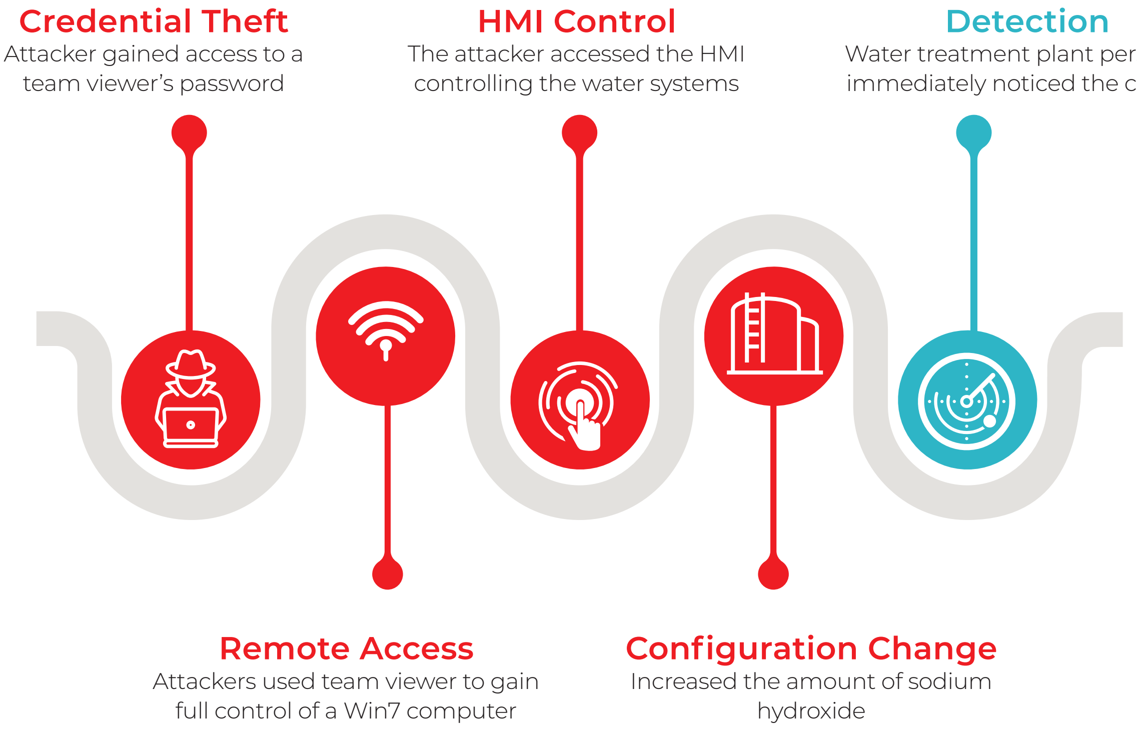

Credential Theft
Attacker gained access to a team viewer's password
HMI Control
The attacker accessed the HMI controlling the water systems
Detection
Water treatment plant personnel immediately noticed the change
Remote Access
Attackers used team viewer to gain full control of a Win7 computer
Configuration Change
Increased the amount of sodium hydroxide

Diagram 4: Florida water utilities attack timeline

March 2021 also saw the indictment[10] of the perpetrator in a 2019 cyberattack on the Post Rock Water District in Ellsworth, Kansas. The small town experienced a cybersecurity breach that threatened drinking water safety, when a disgruntled former employee remotely accessed and disabled water cleaning and disinfecting procedures.

[9] https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/

[10] https://www.cshub.com/attacks/articles/another-cyber-attack-affecting-water-supply

2.2. Oil, Gas & Energy Utilities

The Energy industry was a target of cybercriminals around the world. Victims include the Netherlands energy supplier Eneco, Brazil's energy utilities Copel and Eletrobras Eletronuclear, British energy giant Npower, and more.

In January 2021, a Brazilian fuel distributor, Ultrapar, halted part of its operations at some subsidiaries due to a cyberattack. It took almost two days to restore the company's operations.

In February 2021, a targeted campaign conducted by China-linked group RedEcho against the Indian Power Sector was revealed[11]. Ten distinct Indian power sector organizations, including four of the five Regional Load Dispatch Centers (RLDC) responsible for operation of the power grid through balancing electricity supply and demand, were targeted in the concerted campaign against India's critical infrastructure. Other targets identified included two Indian seaports.

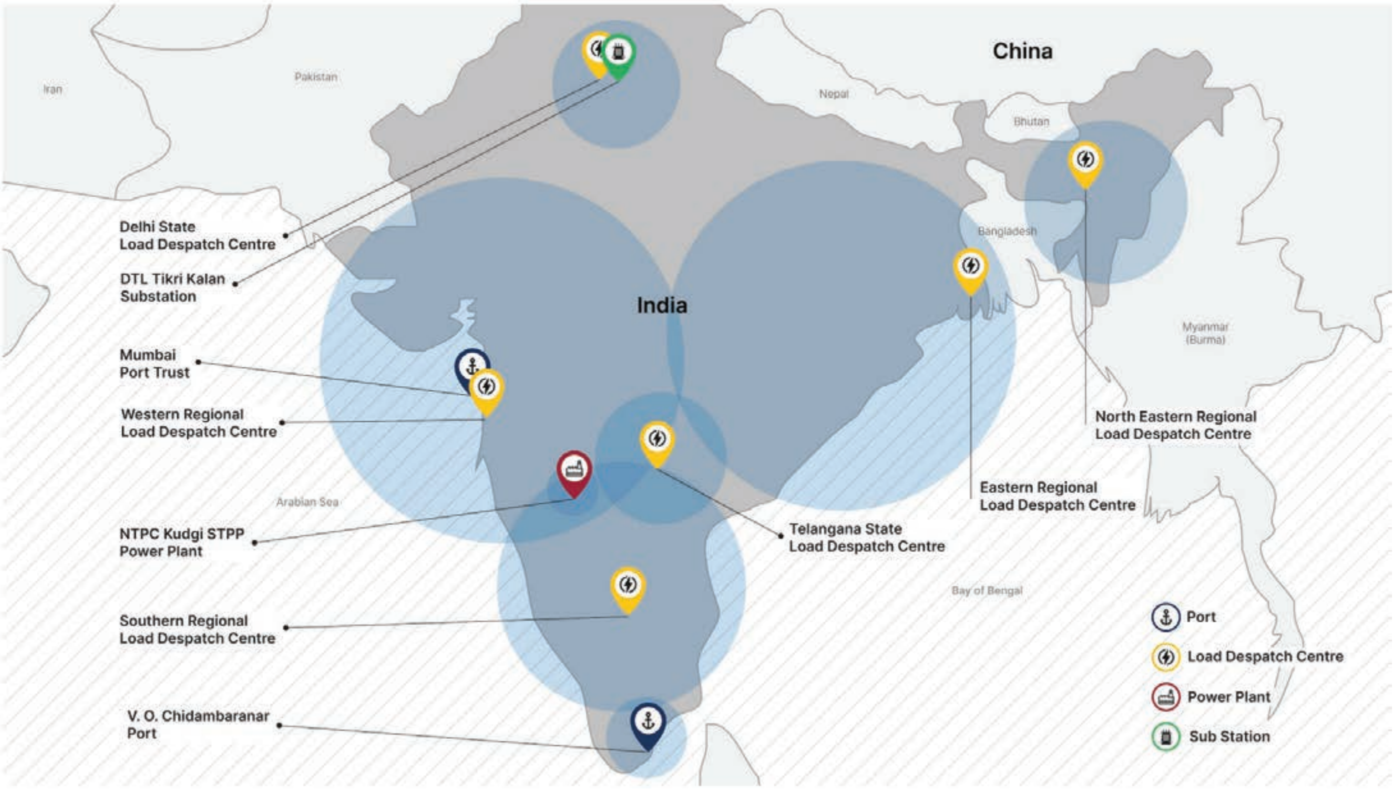

China
Iran
Pakistan
Nepal
Bhutan
Bangladesh
India
Myanmar (Burma)
Arabian Sea
Bay of Bengal
Delhi State Load Despatch Centre
DTL Tikri Kalan Substation
Mumbai Port Trust
Western Regional Load Despatch Centre
NTPC Kudgi STPP Power Plant
Southern Regional Load Despatch Centre
V. O. Chidambaranar Port
Telangana State Load Despatch Centre
Eastern Regional Load Despatch Centre
North Eastern Regional Load Despatch Centre
Port
Load Despatch Centre
Power Plant
Sub Station

Diagram 5: Suspected Indian power sector victims of RedEcho targeted intrusions.
Image source: Recorded Future, Map data ©2021 Google[11]

[11] https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf?utm_medium=email&_hsmi=110851062&_hsenc=p2ANqtz-_h_gWRGCERHb5fl7kUJUCiR7pFoc-gktt3hejdD0XyXQj2uMMm0Jlo8jvdYiKaU43TFvWIR6Hn7O8dpkkrOBG9pXgHNQ&utm_content=110851062&utm_source=hs_automation

2.3. Maritime Ports

Although no major attacks have yet come to light in 2021, maritime trade remains a prime target for cyberattacks and is on the radar of regulators and governments alike. For example, in March 2021 the United States Coast Guard updated its cyber rules to require vessels arriving in US waters to address cybersecurity vulnerabilities within their Vessel Security Assessment no later than December 31, 2021.

The maritime sector is especially vulnerable owing to its dependence on technology for navigation, communication, and logistics. At the same time, both onboard and land-based systems are aging rapidly – a fact exacerbated by the average 25-30 year lifespan of many cargo vessels.

This combination of vulnerability and economic centrality has led to an ever-increasing pace of cyberattacks on maritime vessels and infrastructures. The World Economic Forum cited cyberattacks on transportation infrastructures as the world's fifth highest risk in 2020, and cyberattacks on the maritime sector increased by a staggering 900% over the last three years. Among the targets hit in 2020 were the UN Maritime Agency, shipping giant MSC, and French container transport company CMA CGM.

Cyberattacks On The Maritime Sector

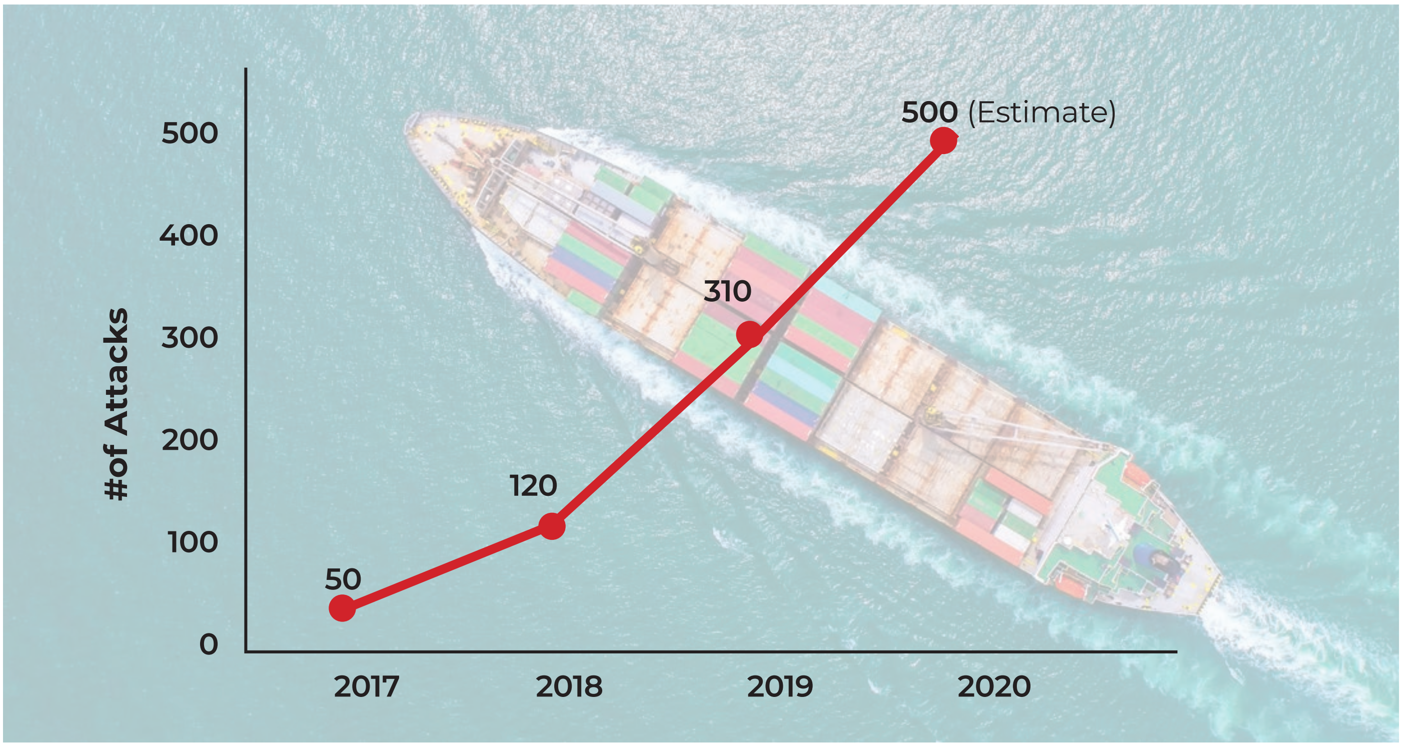


Diagram 6: Number of cyberattacks on the maritime sector over time [14]

[14] https://www.maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise

2.4. The Automotive Industry

Automakers and the automotive industry seem to be getting special attention from ransomware threat actors. One possible reason? Attackers have identified the automotive segment as more vulnerable than others, and they are exploiting it.

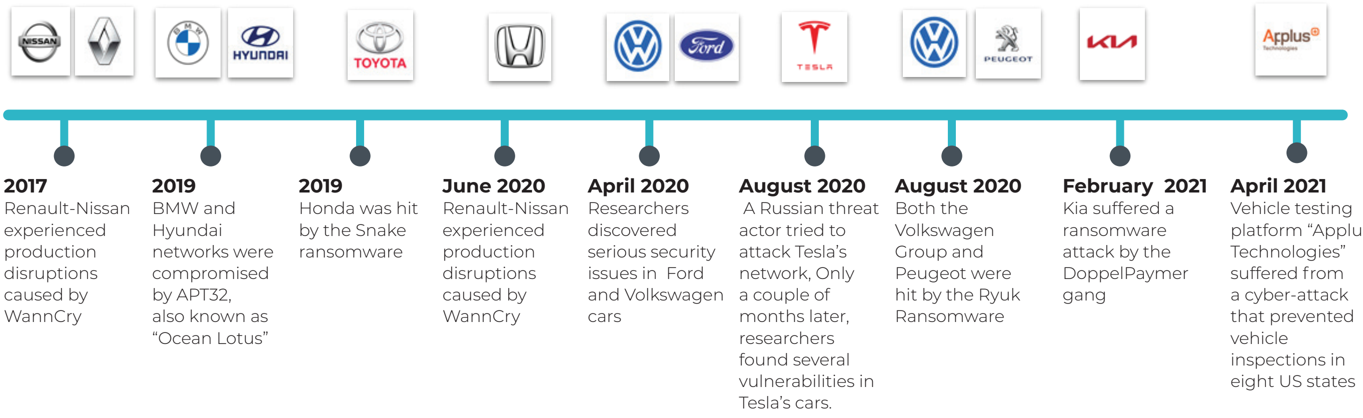
Ransomware threat actors are increasingly adopting more sophisticated techniques to threaten manufacturing operations as a whole, and the automotive segment in particular.

In February 2021, KIA was reported[15] to have suffered from a cyberattack by the DoppelPaymer gang and as a result experienced operational disruption, including disruption of their in-vehicle OEM infotainment and telematics service, UVO. Hyundai Motor America, Kia's parent company, was also affected by the attack.

In March 2021, a cyberattack on Applus Technologies' vehicle emissions testing platform prevented vehicle inspections in eight US states for at least two weeks.

These recent attacks are not the first targeting the automotive industry. Some of the largest names in the industry have been targeted in recent years. The Ryuk ransomware hit both the Volkswagen Group and Peugeot in August 2020, and that same month a Russian threat actor tried to attack Tesla's network. In June 2020, Honda was hit by Snake ransomware...and the list goes on.

Criminals have clearly set their sights on the automotive industry because they understand that manufacturers and service providers can't afford any operational disruption. They also understand that the automotive industry is one of the leading sectors in digitization and automation, making it more vulnerable to cyberattacks.



2017
Renault-Nissan experienced production disruptions caused by WannCry

2019
BMW and Hyundai networks were compromised by APT32, also known as "Ocean Lotus"

2019
Honda was hit by the Snake ransomware

June 2020
Renault-Nissan experienced production disruptions caused by WannCry

April 2020
Researchers discovered serious security issues in Ford and Volkswagen cars

August 2020
A Russian threat actor tried to attack Tesla's network, Only a couple of months later, researchers found several vulnerabilities in Tesla's cars.

August 2020
Both the Volkswagen Group and Peugeot were hit by the Ryuk Ransomware

February 2021
Kia suffered a ransomware attack by the DoppelPaymer gang

April 2021
Vehicle testing platform "Applus Technologies" suffered from a cyber-attack that prevented vehicle inspections in eight US states

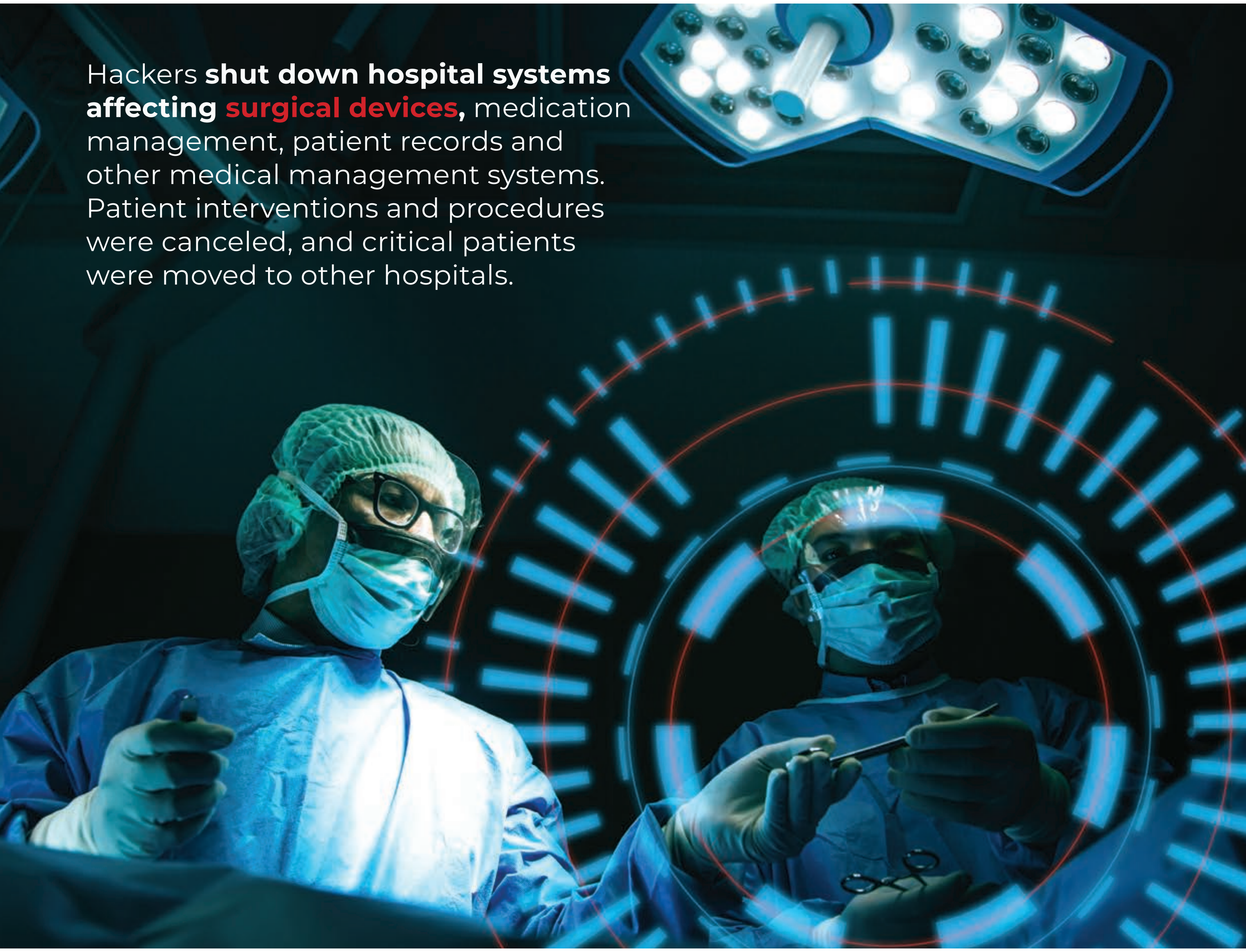
Diagram 7: Cyberattacks targeting the automotive industry

[15] https://www.otorio.com/blog/kia-ransomware-part-of-an-automotive-cyberattacks-trend/

2.5. Healthcare

As global healthcare systems start to see the light at the end of the Covid-19 tunnel, cybercriminals continue to target operational systems in healthcare organizations – slowing response to the pandemic and interfering with patient care.

By way of example, the Dax Hospital in southwestern France was hit[16] by a ransomware attack on February 9. Then, on February 15, a similar attack struck a hospital[17] in Villefranche-sur-Saône, near Lyon. Both attacks used the Ryuk ransomware. These facilities were literally paralyzed by the attacks after categorically refusing to pay the ransoms. Hackers shut down hospital systems – affecting surgical devices, medication management, patient records and other medical management systems. Patient interventions and procedures were canceled, and critical patients were moved to other hospitals.



Hackers **shut down hospital systems affecting surgical devices,** medication management, patient records and other medical management systems. Patient interventions and procedures were canceled, and critical patients were moved to other hospitals.

[16] https://cyberguerre.numerama.com/10288-la-cyberattaque-contre-lhopital-de-dax-a-tous-les-symptomes-dun-ransomware.html

[17] https://www.lemondeinformatique.fr/actualites/lire-le-ransomware-ryuk-traumatise-l-hopital-de-villefranche-sur-saone-81988.html

3. Production and Operations Disruptions

Rather than settling for 'just' data theft, cybercriminals are escalating their attempts to disrupt production by preying on production floors and backup systems. This in turn leads to revenue loss and potentially substantial production recovery costs.

Since January 2021, attackers have managed to physically disrupt the operations of several large manufacturing plants:

- In January, the paper and packaging giant WestRock Co fell victim to a ransomware attack. The attack[18] caused severe disruption in the company's production and shipping capabilities, and the company's stock dropped by 11% in just a week as a result.
- In March, A cyberattack disrupted brewing operations and shipments of the multinational drink and brewing company Molson Coors[19]. As of April 2021, the company was still working on getting its systems back up.
- Police investigated a cyberattack on German paint manufacturer Remmers[20] that shut down a large part of the company's production in March 2021.
- Also in March, Sierra Wireless fell victim to a ransomware attack that halted production at its manufacturing sites. The company's website and other internal operations were also disrupted by the attack.
- In April 2021, a ransomware attack shut down Poker machines at two casinos in Tasmania, Australia, leaving the machines offline during the Easter weekend.
- Also in April, the Cring ransomware caused a temporary shutdown of live production sites in Europe.

[18] https://securityaffairs.co/wordpress/114265/malware/westrock-ransomware-attack-production.html

[19] https://www.forbes.com/sites/leemathews/2021/03/14/cyberattack-disrupts-operations-at-molson-coors/?sh=4ffa2a341bf5

[20] https://www.databreaches.net/de-police-are-investigating-a-cyber-attack-on-paint-manufacturer-remmers/

4. Vulnerabilities and Exploits

4.1. VPN Exploited

VPN solutions are only as secure as their weakest link. Attackers often exploit vulnerabilities in VPN solutions to gain remote access to operational networks. A recent example is the Cring ransomware, which was used in a series of attacks against industrial targets and control systems (ICS) by exploiting Fortinet's VPN server.

The Attackers exploited CVE-2018-13379, a vulnerability in FortiGate SSL VPN servers, to gain access to the victims' networks. The vulnerability allows unauthenticated attackers to obtain a session file that contains the username and plaintext password for the VPN. Victims to date are mostly industrial enterprises in Europe. In at least one case, Cring caused a temporary shutdown of a live production site. Reports[21] raise concerns about the reasons that facilitated these incidents - including the use of unpatched devices, lack of updated databases, poor permissions management, lack of segmentation of the network, and more.

Another loophole in VPN solutions is that they can be used by malicious insiders to attack their organization's network remotely. Malicious insiders are often unhappy current or former employees, who retain access to sensitive networks. The users can cause extensive damage through privileged misuse.

As mentioned above, in April 2021, a former employee of Post Rock Water District in Ellsworth, Kansas was charged for remotely accessing one of a water treatment's computers, over two months after he resigned, and shutting down the cleaning and disinfecting procedures that make water potable.

This is not the first case of a former employee using unrevoked remote access privileges to damage operational systems. As early as 2014, a former employee of Georgia-Pacific, a paper maker, used his active VPN connection to access the company's servers and interfere with industrial control systems (ICS) in the plant for two weeks.

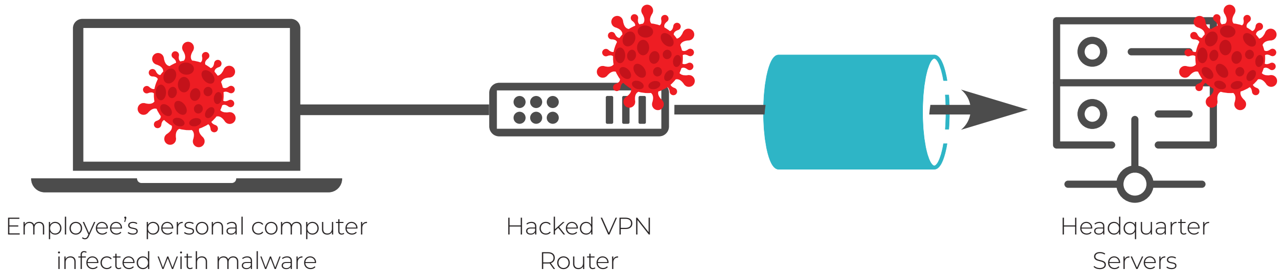


Diagram 9: VPN Vulnerabilities exploitation

[21] https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Vulnerability-in-Fortigate-VPN-servers-is-exploited-in-Cring-ransomware-attacks-En.pdf

4.2. Remote Access Vulnerabilities

As mentioned earlier in this report, over the first quarter of 2021, more than 52 new vulnerabilities were disclosed and reported in industrial automation and control systems.
The vulnerabilities were discovered in products from industrial giants such as Siemens, Schneider Electric and TRUMPF well as smaller industrial manufacturers such as Pepperl+Fuchs and mbConnect. The 2020 rise in the number of vulnerabilities in automation software, as well as supervisory and remote access solutions, continues in 2021.

In Q1 2021, OTORIO's Pen-Testers found more than 20 critical security flaws in a popular industrial remote access solution, mbConnect. Attackers can take advantage of these vulnerabilities to cause severe damage, including:

- Blocking remote access to hundreds of different mbConnect customers' production floors by causing a denial of service in mbConnect devices.
- Exfiltrating sensitive customer information and personal data.
- Accessing mbConnect's sensitive data, including source code, SQL files, and script files.
- Controlling web pages in mbConnect's website, facilitating targeted phishing attacks to steal mbConnect's customers' credentials. Attackers can use such stolen credentials to connect to customer production floors and cause severe damage.

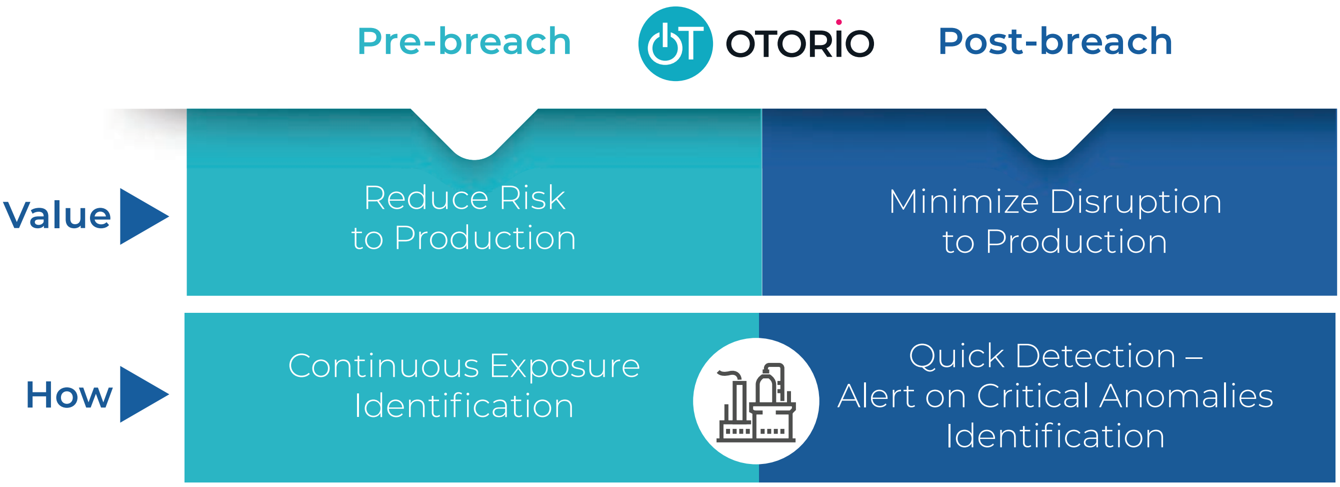
more than **52 new vulnerabilities** were disclosed and reported in industrial systems

5. 2021: More Challenging than 2020?

As we have learned in this report, when it comes to cyberattacks, 2021 is shaping up to be at least as challenging for manufacturers and critical infrastructure utilities as 2020 was, if not more so.

This makes it more important than ever to understand the differences between OT and IT cybersecurity – vastly different fields. IT cybersecurity specializes in securing bits and bytes – crucial for the administrative side of any business. OT cybersecurity, on the other hand, specializes in securing both data and physical systems.

It is important to choose a cyber defense approach that specifically fits OT environment needs. OTORIO recommends combining a traditional reactive approach with a proactive risk reduction approach. Proactive solutions should focus on pre-breach risk reduction activities including continuous exposure identification and mitigation. Reactive solutions should focus on post-breach minimization of disruption to production, relying on quick detection and response. You can read more about this approach in OTORIO's blog post "The Two Sides of the OT-Security Equation".



Pre-breach
OTORIO
Post-breach
Value
Reduce Risk to Production
Minimize Disruption to Production
How
Continuous Exposure Identification
Quick Detection – Alert on Critical Anomalies Identification

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