INDUSTRIAL CONTROL SYSTEM
ICS STRIVE
COVERING SECURITY, THREATS, REGULATIONS, INCIDENTS, VULNERABILITIES WITH EXPERTS

WATERFALL®
Stronger Than Firewalls

OT Security Incidents

2021 Trends and Analyses

Andrew Ginter
VP Industrial Security
Waterfall Security Solutions

Greg Hale
Editor & Founder
Industrial Safety & Security Source

OT Security Incidents in 2021: Trends & Analyses

Andrew Ginter,
VP Industrial Security | Waterfall Security Solutions

Greg Hale,
Editor/Founder | Industrial Safety and Security Source

The year 2021 saw the number cyber attacks with physical consequences in process and discrete manufacturing industries more than double over those reported in 2020. These attacks were in addition to significant numbers of attacks with physical consequences in healthcare, education and other industries. Almost all these incidents were the result of targeted ransomware. Almost all these attacks impacted multiple physical sites.

These findings and others in this report are the result of Waterfall Security Solutions' cooperation with ISSSource in analyzing 2021 data in the ICSSTRIVE.com OT cyber incident database. The database records and categorizes public reports of OT incidents. This report is focused on cyber incidents with physical consequences in:

- Discrete manufacturing sites – sites that combine small parts into larger manufactured objects, such as automobiles, consumer goods, and industrial equipment, and
- Process industry sites – electric power, oil & gas, human consumables, rails, shipping, mining and many other industries where physical operation can be modelled as a continuous process, rather than assembling discrete components.

While these industries are the focus of this report, we also touch on physical consequences of cyber compromise in other verticals where there are high volumes of such attacks: casinos, healthcare and education. In the first section of the report we present the raw data and in the second section we look at trends, project those trends into the future and make recommendations for improved OT cyber risk management programs.

2021 Data

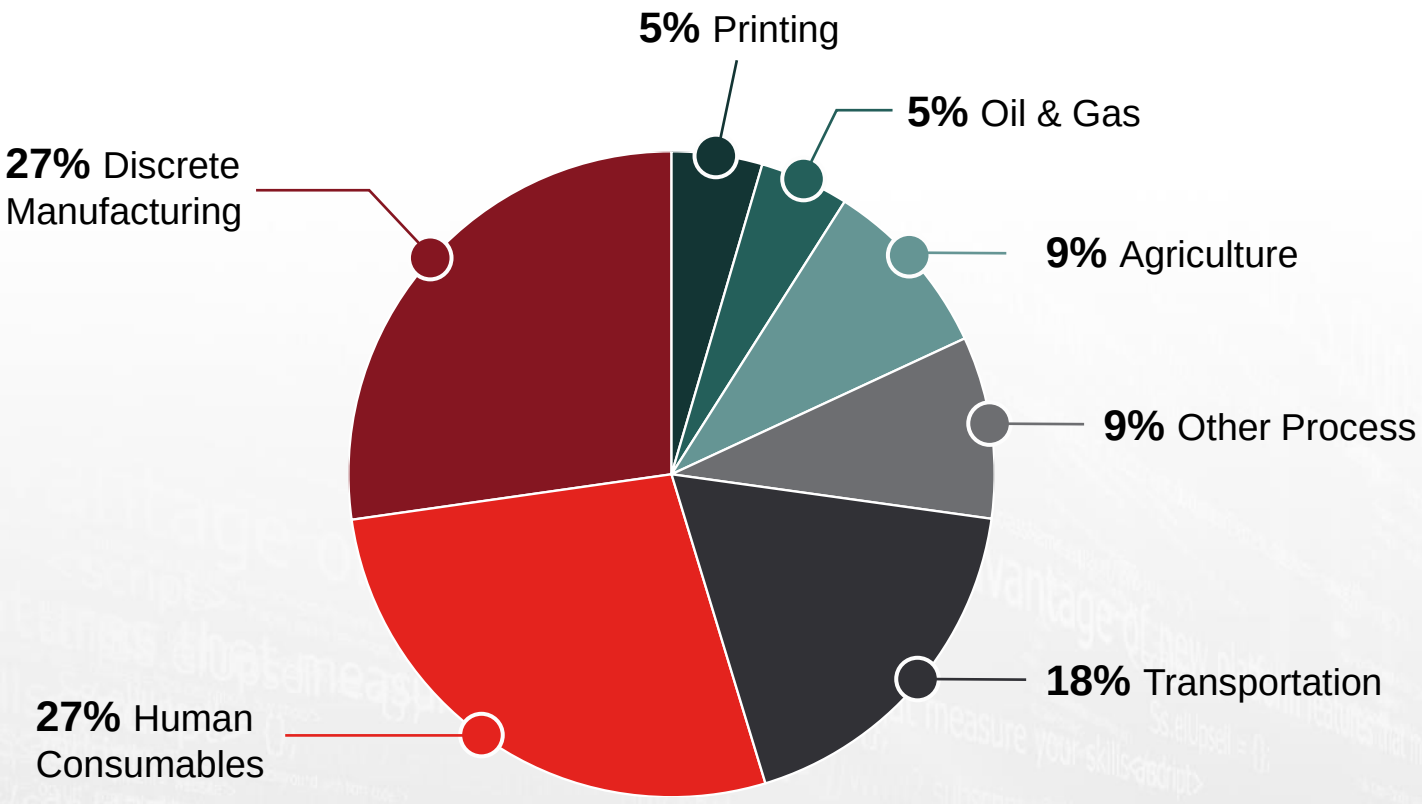
OT OUTAGES

Out of 64 incidents reported in 2021, 22 were cyber attacks with physical consequences in discrete manufacturing and process industries. These attacks represent a 144% increase over such incidents in 2020.

2021	Ind	Notes
Jan	Discrete	**Palfinger** – lost almost 2 weeks crane production at all plants
Jan	Process	**Westrock** – reduced packaging production by 85,000 tons
Feb	Discrete	**Beneteau SA** – boatmaker suffered 3-4 week shutdown at several manufacturing plants
Mar	Discrete	**AmsteelFlash** – multiple printed circuit board plants shut down
Apr	Transport	**Bakkier Logistiek** – disrupted ability to take new orders, delaying shipments to retail outlets for 5 days, causing retail shortages of packaged cheese
May	Human Consum	**Molson Coors** – disrupted brewery operations, production and shipments, delaying $120-$140m in earnings
May	Discrete	**Sierra Wireless** – halted production at all manufacturing sites
May	Process	**Ardagh Group** – shipping delays to glass products cost $34m
May	Oil & Gas	**Colonial Pipeline** – 6 days downtime for largest gasoline pipeline in USA, triggering widespread gasoline shortages in US Northeast
May	Human Consum	**JBS SA** – several large meatpacking plants shut down
Jul	Transport	**Iran rails** – targeted passenger rail signage causing “unprecedented chaos”
Jul	Transport	**Transnet** – port operator halted operations and declared Force Majeure
Sep	Discrete	**Weir Group** – suffered disruptions to manufacturing & shipping – estimated 20-30m BP impact
Sep	Agriculture	**New Cooperative** – brief interruption to grain receipts and shipments as they switched to manual receipts
Sep	Agriculture	**Crystal Valley Cooperative** – unable to mix fertilizer or fulfil orders for feed for 4 days, switched to manual ops for receiving grain
Oct	Human Consum	**Schreiber Foods** – large cream cheese manufacturer shut down production for days
Oct	Human Consum	**Ferrara** – candymaker suffered production shutdowns
Nov	Human Consum	**Damm Brewery** – halted production (impacted bottling)
Nov	Discrete	**Madix** – halted the manufacture of store fixtures at several sites
Nov	Transport	**Diamond Comic Book Distributors** – suffered 2-4 day delays of scheduled shipments to retailers
Dec	Printing	**Amedia** – publisher missed one and a half days printing
Dec	Human Consum	**Nortura** – food producer halted production at several sites

Attacks with OT Consequences in 2021

Out of 64 incidents reported in 2021, 22 were cyber attacks with physical consequences in discrete manufacturing and process industries. These attacks represent a 144% increase over such incidents in 2020.



Attack Distribution by Industry

Ransomware was responsible for 21 of all 22 incidents. In other words, ransomware was the cause of all incidents with physical consequences, except for the July rails incident in Iran. OT ransomware incidents with physical consequences have thus increased 133% year-over-year from 2020, up from 9 in 2020. In addition, most of these attacks affected multiple sites. Published estimates of damage ranged up to $140m per incident.

Note that these numbers all represent lower bounds, because the ICSSTRIVE database is based on public reports. There may have been public reports of incidents that were missed in the database. There may have been incidents that were not reported in public media and there may have been physical consequences that were not reported for incidents that were reported.

NEAR MISSES

In addition to incidents with physical consequences, there are noteworthy “near misses” in the data set – incidents that had the potential for physical consequences if the circumstances of the attack had been slightly different.

In addition to incidents with physical consequences, there are noteworthy "near misses" in the data set – incidents that had the potential for physical consequences if the circumstances of the attack had been slightly different.

2021	Ind	Notes
Jan	Water	**Oldsmar Water Treatment** – An attacker used an obsolete TeamViewer account to operate the HMI to increase lye concentrations in finished water – the attempt was thwarted by an observant operator
Jun	Process	**Fujifilm** – Ransomware caused delays in receiving orders for COVID19 test kits, but no product shortages due to the attack were reported
Jul	Water	**Limestone Water & Sewer District** – Ransomware impaired the alarm system that reports over-heated pumps and over-filled reservoirs, but no physical equipment damage or spills were reported
Jul	Transp	**Northern Train** – Ransomware cripples self-serve ticketing kiosks, but customers were able to continue purchasing tickets in other ways
Oct	Transp	**Danos Management Consultants** – Ransomware "leaks" into shipping networks crippling communications with ships at sea –shipping firms fell back to emergency communications
Oct	Transp	**Toronto Transit Commission** – Ransomware crippled the main communications system – transit busses reverted to emergency radio
Nov	Power	**CS Energy** – Ransomware targeted IT and power plants took quick action to "physically separate the two environments," preventing power generation shutdowns
Dec	Transp	Oahu's **TheBus** and **Handi-Van** – Ransomware crippled ride scheduling systems – fell back to telephone-based ride scheduling

OTHER INDUSTRIES

Cyber attacks caused significant physical consequences in other industries as well. All these attacks were either identified as ransomware or were not identified and were presumed to be ransomware. This report does not draw conclusions about these attacks, but for the record, the ICSSTRIVE data set shows:

- Attacks on IT networks at three casino operators caused eight casino sites to shut down for up to two weeks each out of concerns for patrons' privacy.
- Attacks on seven school districts, colleges and universities caused up to four days of cancelled classes each, at times because of impaired smoke & fire detection systems. The attacks also delayed starts to the school year and in one case forced classes to be operated without air conditioning.
- Ten attacks impaired at least 17 hospitals, causing cancelled outpatient visits, rescheduled surgeries and diverted ambulances. At one hospital, ambulances were diverted for four weeks and the total cost was reported to be $113m, before litigation costs.

In most of these attacks, only IT systems were impaired, but still caused shutdowns and other physical consequences.

In addition, two attacks with retail consequences are noteworthy:

- October 2021 – An attack on gas stations in Iran by a presumed hacktivist group crippled the authentication system for government-issued gasoline discount cards. This caused gas stations to close and produced very long line-ups while consumers awaited re-opening.
- July 2021 – Coop, a Swedish grocery chain, closed over 500 stores because cash registers were crippled by the Kaseya cloud-ransomware breach, where a cloud-based security update server was compromised to seed ransomware into over 1000 enterprises at once.

While retail is out of scope for this report, it is worth noting that gas stations are critical retail infrastructure, and that these stations were targeted in a second hacktivist attack on Iran. Grocery stores are also considered to be critical infrastructure and the Swedish Coop grocery chain outage is an example of a disturbing new development – cloud-seeded ransomware.

ANALYSIS

INTENT

Attributing intent to any of these attacks is difficult, as the attackers generally do not tell us what their objectives are and when they do issue statements, one must always bear in mind that these statements are made by criminals and are therefore of questionable accuracy. None the less, we do observe that:

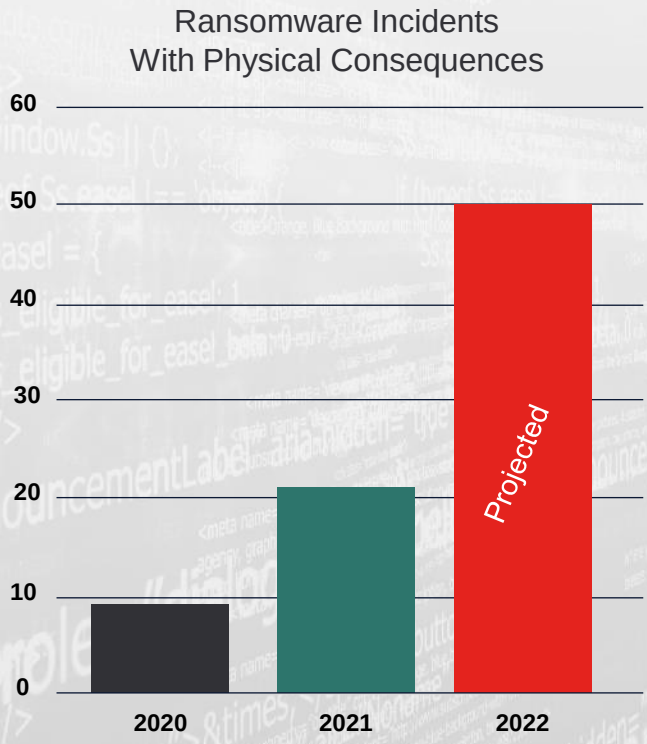
- A statement attributed to the ransomware group behind the Colonial Pipeline attack claimed the group did not intend to cause the outage,
- The hacktivist attacks on Iran's gas stations and rail signage systems were likely to have had the objective of disrupting gasoline purchases and passenger rails traffic, since no ransom demands or other profit motives were reported, and
- The sophistication of ransomware attacks continues to grow as attack groups are targeting specific victims at critical times. For example, in September during the harvest time for many grains, the Iowa agricultural business, New Cooperative, suffered a ransomware attack that impaired many systems, including those used to receive grain at terminals. The attackers demanded a $5.9 million dollar ransom.

More generally, even when physical / OT consequences were not the specific objective of ransomware attacks, it seems likely that ransomware criminal groups were not disappointed with the results of their attacks, since these outcomes increased the likelihood of ransomware payouts.

In the vast majority of these attacks IT assets were reported to be impaired by the attacks, while a minority manipulated or impaired OT assets.

The Colonial Pipeline incident is an example where IT assets suffered the ransomware attack, but the company decided to shut down all of its operations out of caution.

Prediction: Production outages and other physical consequences increase the likelihood that victim organizations will pay large ransoms to attackers. We predict that ransomware-induced outages will triple in 2022 over 2021.



INDUSTRIES

Most of 2021's attacks on industrial sites are reported to have targeted IT networks. World-wide, both IT and OT networks in the Oil & Gas industry have a reputation of being heavily defended, and so it makes sense that there was only a single incident in that industry with physical consequences – the Colonial Pipeline attack. Similarly, the electric sector in North America, and to an extent world-wide, has a reputation as being the most cyber-regulated and secured. It is therefore not surprising that there were no cyber incidents that impaired operations in this sector in 2022.

In transportation, some OT networks also have a reputation for being thoroughly protected, for example passenger rail signalling systems. As a result, the large fraction of incidents in transportation does seem surprising. Not all incidents in transportation were in passenger rails, however, and those that were in this industry tended to target the more exposed ticketing and signage systems rather than the more heavily protected signalling systems.

The ICSSTRIVE database also reports four attacks on water and wastewater facilities in 2021. While the worst consequences of these attacks resulted in only "near miss" categorization, the water sector is traditionally underfunded for cybersecurity. This is an issue, considering the importance of what the sector produces – clean drinking water for citizens.

RANSOMWARE CONSEQUENCES

Data from both 2020 and 2021 suggests three ways that ransomware can cause physical consequences in process and discrete manufacturing industries:

1. Ransomware actors can target OT systems directly, through targeted or supply-chain attacks, resulting in mis-operated or otherwise impaired OT automation and operations,
2. Ransomware actors can target IT systems, indirectly affecting OT systems when victim enterprises shut down physical operations "in an abundance of caution,"
3. Ransomware actors can target and impair IT systems that are essential to second-by-second or minute-by-minute industrial operations.

Few public incident reports include data about why operations were shut down as a result of a ransomware attack. Prudent enterprises must take steps to eliminate the possibility of all three kinds of OT shutdowns due to ransomware attacks.

Prediction: Ransomware groups will target OT networks and services more often and more specifically in 2022 than in 2021. One reason: when the dollar cost, opportunity cost or reputational cost of impaired OT networks is unacceptable, then victim organizations will be more open to paying larger ransoms.

Another reason: targeting OT networks more visibly leads to more victim organizations fearing an OT compromise and shutting down operations out of an abundance of caution when suffering any ransomware attack. Again, this leads to a higher frequency of higher payouts.

CLOUD-SEEDED RANSOMWARE

In July 2021, a ransomware group exploited a Kaseya cloud service to distribute ransomware to over 1000 organizations in the space of 45 minutes. No impacts on process or discrete manufacturing industrial operations were reported, though 500 grocery stores in Sweden shut down for two days because their cash registers were crippled.

The attack highlights the risk of cloud-connected infrastructure. In the terminology of the Industrial Internet Consortium's Security Framework, industrial Internet systems consist primarily of edge devices connected directly or indirectly to cloud services. In this terminology, all connections from equipment on ICS / OT networks out to Internet services of any sort constitute cloud connections. This is especially true of any such service that is able to update software or firmware in edge devices, or otherwise control the behavior of such devices.

Too many security practitioners focus on encryption and data privacy capabilities when evaluating the security of cloud providers and the wisdom of connecting physical operations to cloud systems. Too many practitioners fail to consider, or discount the possibility, that cloud providers themselves may be compromised, and that attacks may pivot through compromised cloud services into physical operations inside of encrypted cloud connections.

Prediction: Cloud-seeded ransomware is very profitable because it attacks hundreds or thousands of victim organizations at once. We should prepare for more attacks like this one in the future.

And, because critical infrastructure enterprises are more likely than not to pay a ransom, we should expect cloud-seeded ransomware to target industrial software providers by the end of 2023.

NATION-STATE ATTACK TECHNIQUES

Looking further back in time, we observe that:

- Targeted attacks, where a Remote Access Trojan is planted in a victim's network and operated by remote control, became common knowledge in 2006-7 and were widely attributed to Chinese intelligence agencies and their contractors. These attacks came into widespread use by criminal groups by 2013-2014.
- Cloud-based attacks, where malware disguised as a security update is distributed through cloud services, became common knowledge with the NotPetya attack in 2017. That attack was attributed to Russian intelligence agencies, or their contractors. The first such attack by ransomware actors was the Kaseya attack in 2021, impacting over 1000 victim businesses in 45 minutes.

We conclude that for important attack patterns, criminal groups lag nation states by 4-5 years. Attack campaigns we see nation-states conducting today, we should expect to see criminal groups using against all of us within a very few years time.

Prediction: Today, we see nation-states breaching VPNs and two-factor authentication – think the Pulse Secure attack.

We predict that before 2025, we will see ransomware actors doing the same to deposit Remote Access Trojans into victim organizations.

RECOMMENDATIONS

GOAL - CONTINUOUS OPERATIONS

In May 2021, the entire Colonial Pipeline shut down for 6 days because the company's IT network was crippled by ransomware. The societal impact was significant, since the pipeline supplies a large fraction of all gasoline consumed in the East Coast of the United States. A month after the event, the US Transportation Security Administration (TSA) issued a confidential directive to the nation's largest petrochemical pipelines. A redacted version of the directive was subsequently published by the Washington Post in response to a Freedom of Information Act request. The driving imperative for the directive is arguably requirement II.B.2(b), which mandates:

> *"Implement network segmentation sufficient to ensure the Operational Technology system can operate at necessary capacity even if the Information Technology system is compromised"*

IT networks are much more exposed to ransomware attacks than OT networks should be, and so it is reasonable to expect that IT networks will be breached much more frequently than OT networks. Thus for critical infrastructures and indeed for many industries, the TSA requirement captures an important goal for resilient OT security planning: design our automation so that our physical and manufacturing operations can continue running safely and continuously, even when the more-exposed IT network is compromised.

SECURE OPERATIONS TECHNOLOGY

Secure Operations Technology (SEC-OT) is the methodology used by secure sites to achieve this goal of safe, continuous and correct operation. When applied to the problem of nation-state-grade ransomware, two elements of the methodology stand out.

The first element is managing attack information flows. When modern ransomware groups target physical operations directly, they insert their malware directly into industrial control networks and operate the malware there by remote control. Similarly, when a ransomware attack triggers a shut-down of operations "in an abundance of caution," the victim enterprise decides to shut down operations pre-emptively. The solution in both cases is to control attack information flows so thoroughly that the movement of attack information into operations networks, either deliberately or accidentally, is practically impossible.

SEC-OT information flow controls, such as removable media controls, removable device controls and unidirectional gateway technology, make the movement of attack information into operations networks from external sources practically impossible. With strong SEC-OT protections in place, ransomware attacks, even those using nation-state attack tools and techniques, cannot reach the industrial control systems operating physical infrastructures and manufacturing processes, and so cannot cause the malfunction of these processes.

ELIMINATING IT DEPENDENCIES

The second element of the SEC-OT methodology that is relevant to the majority of 2021's ransomware attacks has to do with OT/control system dependencies on IT systems and services. A vital tenet of SEC-OT is that all systems and data that are essential to second-by-second and minute-by-minute physical operations must be hosted in the operations or manufacturing network and must be protected according to the principles of the SEC-OT methodology.

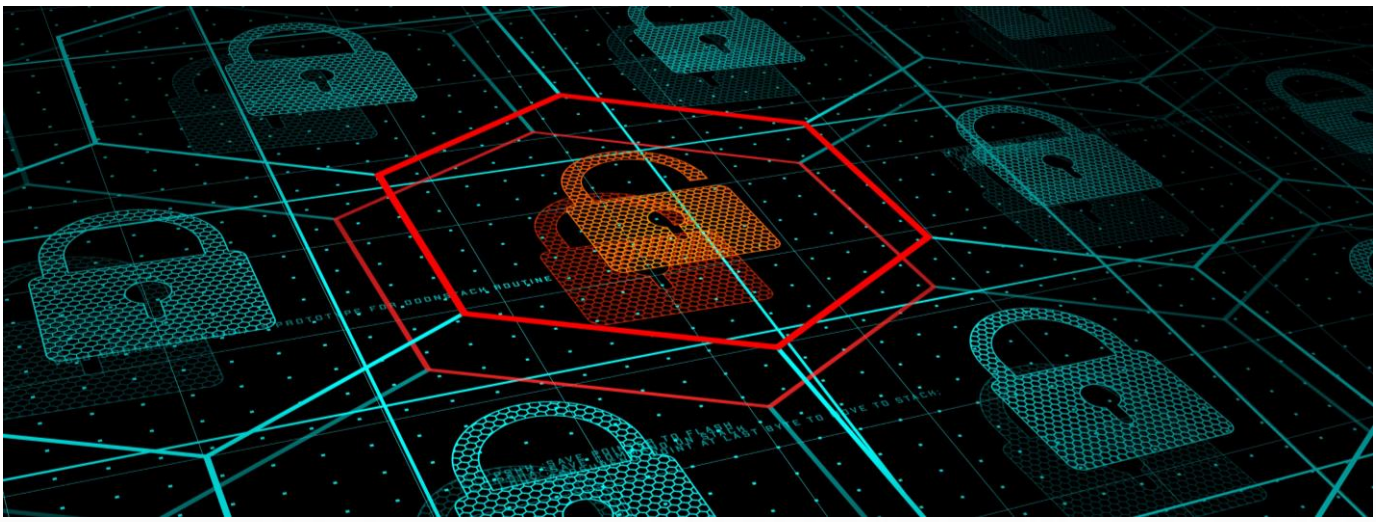
For example, if an otherwise well-defended industrial system depends on an IT-resident Windows Domain Controller to manage permissions, then a ransomware attack that cripples this IT system will force a shut-down of industrial control systems as well. When an enterprise chooses to use a Domain Controller in operations, the SEC-OT methodology demands that this controller be entirely resident in the protected OT network, rather than the Internet-exposed IT network.

Or, if a factory executes a set of production orders from an IT Enterprise Resource Planning (ERP) system, and stops when no new production orders are available, then crippling the IT network and the ERP system will cause the factory to stop as soon as the current set of production orders is completed. To ensure continued manufacturing operations even when ransomware cripples the IT network, such a factory must store a queue of production orders that add up to one or two weeks of operations – for as long as a clean-up of the IT network will take.

CLOUD DEPENDENCIES

Controlling dependencies on cloud services deserves special mention. Ransomware delivered through cloud services can cripple not just one factory or physical operation, but all operations that use the compromised cloud service, enterprise wide. Preventing such compromise is straightforward – secure sites enjoy the benefits of industrial cloud services, safely, by connecting to those services only via unidirectional gateways.

Unidirectional gateways include hardware that is physically able to send information in only one direction, from the industrial operation out to the cloud. When the only connection from an industrial system to a cloud service is via such a gateway, no attack on the cloud service, no matter how sophisticated, can leak back into physical operations.



CONCLUSIONS

Ransomware and other cyber attacks that shut down or otherwise impair physical operations are increasing at a rapid pace. Worse, today's ransomware groups are trailing nation-state attack tools and techniques by only about half a decade. This report predicts that within the next 2-3 years, cloud-seeded ransomware and two-factor authentication bypass attacks will pose very serious threats to critical infrastructure organizations and to manufacturers of all types. A more potentially dangerous supply chain attack such as the SolarWinds attack could lead to a compromise of thousands of organizations to the point of falling victim to ransomware or worse.

Classic approaches to IT security (IT-SEC) are not enough to assure safe and continuous physical operations when IT networks end up breached. In 2021 the world saw 22 attacks with physical consequences documented in the popular press, for process and discrete manufacturing industries. Ransomware attacks on IT networks in other kinds of enterprises numbered in the thousands. Every one of these attacks defeated IT-SEC class security measures. If we wish to avoid our physical operations being crippled by attacks on our IT networks, then we need stronger protection. We need the operation of our OT networks to continue unimpeded for at least as long as it takes for us to restore essential functionality to our IT networks.

TO DIG DEEPER

Waterfall Security Solutions continues to make the defining text on the SEC-OT methodology - *Secure Operations Technology* – available free of charge, as a public service to the industrial security community. To request your copy, visit https://waterfall-security.com/sec-ot

For a deeper look at cyber attacks with physical consequences and how to design defenses to defeat those attacks, you can download The Top 20 Cyber Attacks on Industrial Control Systems at https://waterfall-security.com/top-20

To see the latest OT security incidents with physical consequences, click on the ICSSTRIVE website at https://icsstrive.com

For all the latest news on industrial safety and security, click on Industrial Safety and Security Source at https://isssource.com or subscribe to The Shield weekly newsletter.

ABOUT WATERFALL

Waterfall Security Solutions is the OT security company, producing a family of Unidirectional Gateway technologies and products that enable safe IT/OT integration, enterprise-wide visibility into operations, and disciplined control. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off-shore and on-shore oil and gas facilities, manufacturing plants, power, gas and water utilities, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases, and protocols in the market. For more information, visit www.waterfall-security.com.

ABOUT ISSSource

Industrial Safety and Security Source provides independent and unbiased automation, safety and security information for manufacturing and automation professionals. Our newsletter The Shield provides timely updates. Our incident repository ICSSTRIVE.com is focused on industrial cyber incidents in the public record. Our podcast Today with ISSSource provides insights, analysis and predictions from leaders in the industry. For more information, visit www.isssource.com.