WATERFALL®
Stronger Than Firewalls

OT/ICS Ransomware in the Supply Chain: Learnings from Attacks in 2020

Andrew Ginter,VP Industrial Security
Waterfall Security Solutions

Table of Contents

Executive Summary

2020 was not a good year for cyber attacks on industrial control systems (ICS) and operational technology (OT) networks:

- Targeted ransomware: Nine attacks shut down physical operations at industrial sites – all were targeted ransomware.
- SolarWinds Orion: The single biggest cyber attack in history – the SolarWinds Orion supply chain breach – impacted as many as 18,000 organizations, many of which were industrial enterprises with physical operations.

In addition, ICS and OT networks are increasingly connected, both to enterprise networks and to Internet-based cloud providers in the Industrial Internet of Things (IIoT) configurations. Such connectivity makes targeted and supply chain attacks ever simpler and more far-reaching in their consequences.

In 2020, ransomware, targeted ransomware, supply chain breaches and cloud connectivity all emerged as top-of-mind concerns for security teams at industrial enterprises. Security teams responsible for industrial operations are re-evaluating their security programs in light of this new, pervasive threat environment.

To accelerate such evaluations, this report describes four representative and credible threats for 2021 and beyond – pervasive threats that all ICS / OT security teams should consider going forward. Each threat is evaluated against three different kinds of widely-recommended security postures.

	Software-Based Protection	Software + Monitoring & IDS	Unidirectional Protection
Ransomware Time Bomb	✖	✖	✓
Targeted OT Ransomware	✓[1]	✓[1]	✓
OT Management Ransomware	✖	✖	✓
Cloud / IIoT Ransomware	✖	✖	✓

[1] Software-based protections would not, however, protect against straightforward variations of this attack.

For each attack and security posture, variations that may affect the outcome of the evaluation are also considered. We conclude that, given the pace of evolution of the pervasive threat environment, industrial enterprises will benefit from unidirectional protections at their IT/OT interfaces.

Introduction

Industrial Control System (ICS) and Operations Technology (OT) cybersecurity practitioners are looking back at 2020 to see what can be learned from the SolarWinds Orion/Sunburst breach and from targeted ransomware attacks. In 2020, all published cases of cyber attacks impairing physical operations were targeted ransomware. Then, late in the year, the SolarWinds supply chain breach impacted up to 18,000 organizations, with up to 200 of those organizations being targeted specifically through the Sunburst malware.

In addition, ICS and OT networks are increasingly connected, both to enterprise networks and to Internet-based cloud providers, because of Industrial Internet of Things (IIoT) deployments. Such connectivity makes targeted and supply chain attacks ever simpler and more far-reaching in their consequences. ICS and OT security programs are currently being re-evaluated at many industrial enterprises in light of these developments in the pervasive threat environment.

SolarWinds Orion / Sunburst

The biggest cyber breach in 2020 was the SolarWinds Orion supply chain breach:

- Two apparently different threat actors covertly inserted two separate remote-control "Sunburst" and "Supernova" malware artifacts into a signed, authorized SolarWinds Orion product update.
- The update was downloaded by over 17,000 organizations, and presumably installed in a large fraction of those organizations.
- The Sunburst malware delayed activation and successfully evaded modern anti-virus systems, intrusion detection systems, "sandboxing" anti-malware scanners and other software-based security systems.
- The malware eventually connected to an Internet-based command and control (C2) server using a benign-seeming HTTPS connection in which C2 traffic was steganographically encoded.
- The threat actors used the malware by remote control through their C2 at up to 200 organizations.

After months of exploits, the malware was eventually discovered and disclosed by FireEye.

By now, OT/ICS security teams all over the world have completed their initial investigations as to whether the breach affected their operations networks. At this writing, no industrial or manufacturing production losses have been disclosed for the breach, but ICS and OT security teams are still concerned. Past software supply chain breaches did, after all, have OT consequences:

- In 2014, the Havex malware was embedded in IT product downloads. Once installed on an IT network, the malware was operated remotely to jump through IT/OT firewalls into OT networks. The malware then gathered OT/ICS process intelligence via OPC servers and reported that intelligence to a C2 server.
- In 2017, the NotPetya malware was embedded in a software update for popular Ukrainian tax software. The malware was auto-installed in a large number of IT networks. In spite of impacting primarily IT assets, the malware triggered industrial and operations shutdowns in many organizatioins. Bllions of dollarsl of cyber insurance claims are still working their way through the courts.

Given these examples of OT-impacting software supply-chain attacks and the very sophisticated Orion breach, OT/ICS teams are studying how OT/ICS security programs must be updated to address this new class of supply chain threat.

Targeted Ransomware

The year 2020 saw nine public reports of industrial process downtime due to cyber attacks. All of these attacks were targeted ransomware. Targeted ransomware emerged in 2020 as the most pervasive cause of process and manufacturing downtime.

Historically, first-generation ransomware spread automatically and demanded a modest ransom for individual encrypted machines. Today's second-generation, targeted ransomware is remotely operated by attack professionals. The attackers dig deep into targeted networks, encrypt the most valuable machines they can find, and demand significant ransoms for the network as a whole, rather than for individual machines. Targeted ransoms are generally greater than $100,000 USD and there are reports of demands of up to $10 million USD.

Target	Plant-Days Lost	Head Office
Picanol	196	Belgium
Steelcase	140	USA
Lion	63	Australia
X-FAB	48	Germany
Fisher & Paykel	25	New Zealand
Tower Semiconductor	18	Israel
Evras Steel	18	UK
Honda	8	Japan
BlueScope Steel	2	Australia

Targeted ransomware in both the IT and ICS / OT space can be very sophisticated. Many of the criminal groups behind the ransomware are today using attack tools and techniques comparable to those used exclusively by nation-states only half a decade ago. It is therefore no surprise that the physical consequences of these attacks are escalating as well. Eight of the nine attacks causing physical shutdowns in 2020 impacted multiple plants simultaneously. Such targeting by organized criminals only makes sense – multiple plants down at once can overwhelm incident response teams and so increases the likelihood of a payout to the criminals.

Cloud Connectivity and IIoT

The continued push towards greater digitalization and operational efficiencies is leading to ever-increasing enterprise network and cloud connectivity for ICS and OT networks. The average industrial site in process industries such as power generation and refining has up to one half dozen connections to Internet-based vendors such as equipment manufacturers and control system software manufacturers. The average manufacturing site has many dozens of such connections, because of the much wider variety of specialized machines and robots used in modern manufacturing. In addition, the vast majority of industrial enterprises in both kinds of industries have been evaluating for several years IIoT deployments where dozens or hundreds of individual devices are connected directly out to the Internet. Many sites have started to deploy these kinds of solutions.

This is of course very concerning security-wise. All connectivity is a potential attack vector. At the very time where the pervasive threat environment for OT/ICS networks is worsening because of very sophisticated attacks, the increase in cloud connectivity in these same networks is reducing the effectiveness of cyber defensive postures.

Adding It Up

Targeted ransomware incidents are increasing rapidly in both IT and OT networks. It seems clear that ransomware will persist as long it is profitable to criminal organizations. The scope of the SolarWinds Orion/Sunburst supply chain incident is staggering - it is arguably the biggest serious cyber breach in history. Put the two together: it is very likely only a matter of time before organized crime decides to make an investment comparable to the SolarWinds breach in order to deliver ransomware to hundreds or thousands of organizations simultaneously. The trend towards increased cloud connectivity at ICS and OT sites will only make this class of attack easier for the criminal groups involved.

All enterprise and engineering security teams tasked with defending ICS and OT networks need to take these developments in the pervasive threat environment into account. To this end, in this report we extend Waterfall's Top 20 Cyber Attacks on Industrial Control Systems report to explore ransomware-centric variations of the Sunburst, NotPetya and Havex attacks. In addition, we postulate a fourth attack that combines ransomware, supply chain and cloud connectivity. We illustrate how to evaluate these new types of attacks and straightforward variations of these attacks in light of widely-used and widely-recommended OT/ICS security approaches.

Supply Chain Ransomware Attacks

In this section, we consider four credible ransomware-centric variations of the Sunburst, NotPetya and Havex attacks, targeting OT/ICS networks.

#1 Ransomware Time Bomb

A moderately sophisticated threat actor breaks into the software update system of an unsophisticated industrial software vendor. The threat actor adds a ransomware executable to a recently-posted ICS security update. Many industrial enterprises demand that their OT/ICS teams download and test new security updates as quickly as possible after the update is released. The testing process is time consuming and expensive, but a large fraction of the vendor's customers manage to test and install the update within two months of the update's release. These tests uncover nothing suspicious.

Ten weeks to the day after the malware was planted in the security update, the malware activates. The malware encrypts all computers on which it was installed and demands a significant ransom for un-encryption. Hundreds of industrial operations are crippled simultaneously. Incident response teams are overwhelmed. As a result, the threat actor is rewarded with a significant number of ransom payments.

This attack uses a compromised software download, as did the 2014 Havex and 2017 NotPetya malware. The attack uses delayed activation to defeat sandboxing and testing, as did the Sunburst malware.

#2 Targeted OT Ransomware

A moderately sophisticated threat actor builds a remote-control "Remote Access Trojan" (RAT). The actor compromises a poorly-secured industrial vendor's website and embeds the RAT in the vendor's most recent security update. Industrial enterprises download the update, test it, and eventually install the malicious update on their OT/ICS networks.

The RAT connects to a C2 on the Internet. The attack team operates the RAT remotely to learn about the compromised OT network. The team eventually plants copies of the ransomware on the most valuable targets in the network. Dozens of machines are encrypted simultaneously, demanding a ransom from the victim. This attack uses a compromised software download and RAT as did the 2014 Havex malware and the 2020 Sunburst malware.

#3 OT / ICS Management System Ransomware

The largest industrial control system product vendors all sell management systems. These systems are most commonly deployed on IT networks to manage all the vendor's installations at all plants and industrial facilities in an industrial enterprise. These systems are widely used, because they significantly reduce the cost and increase the consistency of managing industrial installations. These systems are powerful - they can install new software, uninstall old software, start, and stop industrial servers, and they have many other features. On the other hand, these management systems represent single points of compromise for massive investments in physical infrastructure.

In this attack, a sophisticated threat actor embeds a RAT in a software update for the management server software at a large, widely-used industrial control system. The malware uses techniques comparable to Sunburst to evade anti-virus, sandboxing and network intrusion detection tools.

The RAT is not embedded in the management server software directly, but rather embedded in the management server's client software modules that are installed on enterprise workstations and laptops for the users who use the management server. The RAT is embedded in the client because IT best practice demands that management servers not have access to arbitrary sites on the Internet. Individual users' workstations and laptops, however, almost always have such connectivity and so can be used to funnel the attackers' instructions through an Internet-based C2 into the management system.

Threat actors take control the management server at dozens of industrial enterprises and use the management system to install ransomware on all managed ICS components at all industrial sites in each targeted enterprise. This happens within a small number of days – management servers run on IT networks and are generally managed as IT assets, with aggressive security update installation schedules. Two weeks after the security update issues, the criminal group triggers the ransomware simultaneously in thousands of plants at dozens of enterprises. This overwhelms incident response teams and maximizes the likelihood of large payouts to the criminal organization.

This attack is very similar to the Sunburst breach. The SolarWinds Orion product is itself a management system for firewalls, routers, and many other devices. The product enables remote management, updates, file and script distribution and other control of these devices.

#4 IIoT Ransomware

A sophisticated threat actor compromises a poorly-defended Industrial Internet of Things (IIoT) cloud vendor and gains control of the vendor's firmware update process. The attacker chooses a vendor whose cloud-connected industrial controllers are essential to continuous operation of a given class of industrial process. For example, all the following routinely have connections to vendor clouds:

- Steam, hydro & gas turbine management systems in power plants,
- Robots on assembly lines, and
- Component manufacturing equipment such as packaging, stamping and conveyance equipment.

The threat actor embeds malicious software in a firmware security update. The malware disables all further firmware updates and disables the industrial controllers.

The attacker also takes control of the IIoT vendor’s software update system. Instead of installing the firmware update under the control of the industrial site, the modified update system ignores software update settings and pushes the update immediately to all devices connected to the compromised cloud site.

Thousands of IIoT devices and systems are now disabled and no longer respond to firmware update attempts. Hundreds of production sites are shut down. Again, this overwhelms incident response teams, leading to a significant number of ransomware payments to the criminal organization.

This attack is a software supply chain attack that relies on compromising firmware development and deployment techniques, comparable to the Sunburst and NotPetya attacks.

Defensive Postures

To evaluate the effectiveness of defenses against these attacks, we consider three defensive postures.

Software-Based Prevention

The majority of industrial, operations and manufacturing sites in almost all industries rely heavily on software-based security systems. Best practice software systems can include, wherever practical:

- layers of firewalls,
- encrypted communications wherever practical,
- least-privilege account management,
- complex, frequently-updated passwords,
- security update/patching programs,
- anti-virus systems,
- whitelisting/application control systems,
- servers running as unprivileged users, and
- mandatory access controls wherever supported.

While software-based security programs can use all the above, most do not. The omissions are often because of cost and compatibility issues. Software-based security programs can be complex and expensive, especially the security update programs.

Software-Based + Detection & IDS

A growing number of industrial sites deploy software-based preventive measures with robust security monitoring, including network and endpoint intrusion detection systems. These monitoring systems are designed to detect attacks in progress. These detective measures are generally coupled with practiced OT/ICS incident response teams and OT/ICS backup and configuration management systems. System and configuration backups, however, can be difficult to accomplish comprehensively in OT/ICS networks because of the wide variety of special-purpose devices in those networks.

Unidirectional Protection

Many industrial enterprises deploy unidirectional gateway technologies as preventive measures. The gateways are simple to deploy and are deployed routinely at IT/OT interfaces. Unidirectional gateway hardware is physically able to send information in only one direction, from the OT/ICS network to the IT network. Unidirectional gateway software makes copies of industrial servers. Enterprise users access OT/ICS data in the enterprise copies. In short, the gateways provide enterprise users with access to industrial data, without providing access to industrial systems.

Industrial sites using unidirectional gateway technology generally also use a standard set of secondary controls, according to the Secure Operations Technology (SEC-OT) methodology. The methodology deploys strict controls over any kind of information that enters an industrial/OT network. All online information flows are mediated by unidirectional gateways, while offline flows such as USB drives, vendor laptops and software updates are strictly controlled.

Note that SEC-OT sites generally also deploy a reasonable subset of software-based security controls. Because of the strength of protection afforded by the primary SEC-OT controls, however, SEC-OT sites are generally able to reduce their expenditures on the most complex and most costly of software security mechanisms, such as security update programs.

Evaluating Attacks & Defenses

We now apply each of the hypothetical supply-chain attack scenarios to each of the defensive postures.

#1 Ransomware Time Bomb

Software-protected sites are exposed to attacks that pivot through intermediate systems and firewalls using stolen credentials and known vulnerabilities. Best practice holds that sites with this kind of exposure must download, test, and install vendor security updates promptly. The process is expensive, but compliant sites often install such updates within 1-2 months of release by the vendor. In this attack:

- The malware is not detected by anti-virus systems, because the malware has never been used before in the wild. In addition, the malware was identified as a legitimate executable that was part of a security update.
- Whitelisting/application control systems do not block the malware, because such systems are configured to allow execution of all executables in security updates.
- New configurations for mandatory access control systems are part of the security update, and the ransomware authors provide configurations that permit the encryption operation.
- Passwords and permissions are irrelevant to the attack, since the control system software must have access to read and write important configuration and data files during normal execution, and so the malware has permission to read, write and encrypt these files as well.
- Encrypted communications do not help defeat this attack. The security update itself is likely to have been acquired over an encrypted connection. Cryptosystems encrypt attacks just as readily as they encrypt legitimate security updates.

In short, there is nothing in conventional software security best practices for industrial/OT networks that will defeat this attack.

When we add intrusion detection, incident response and incident recovery mechanisms into the software security program, we have a similar result. There are no network communications associated with this type of attack that an intrusion detection system might detect. A filesystem consistency checking system might detect the changed, encrypted files, but would do so only after the malicious file encryption was already in progress. Worse, investigating these alerts, triggering an incident response team, and investigating the incident all take time. By the time the incident response team is scrambled to the site, the damage is done. While intrusion detection and security monitoring systems do add other kinds of value to OT/ICS security programs, such programs cannot prevent this class of attack.

Unidirectional protections and the SEC-OT discipline are a better way to prevent this attack. Because of strong unidirectional protections for online information flows, and strong offline protections against attacks embedded in USB drives or other offline information flows, SEC-OT sites are not exposed to pivoting or USB attacks. As a result, SEC-OT sites often have 6, 12 or even 18-month security update testing cycles. Slowing down security updates reduces costs at SEC-OT sites, without materially affecting security. This means that any malware or other problems in a security update generally become evident in less-secure sites long before secure sites have completed their testing.

In this attack example, the ransomware triggers while the compromised update is still in the unidirectionally-protected site's isolated test bed. The test bed is easily erased and rebuilt, and there is no effect on physical operations. In summary:

	Software-Based Protection	Software + Monitoring & IDS	Unidirectional Protection
Ransomware Time Bomb	✖	✖	✓

#2 Targeted OT Ransomware

Again, software-protected industrial sites generally must download, test, and install security updates promptly. In the targeted OT ransomware example, the security update includes a RAT that evades sandboxing and activates after the malicious update is installed on the OT network. In a software best practices network, however, firewalls are configured to prevent ICS and OT equipment from connecting to arbitrary Internet servers. This means that in this attack scenario, the RAT's attempt to connect to its C2 server fails. Yes, the malware is still present in the OT/ICS network, but the RAT does nothing until a C2 tells it to do something. In this case, the C2 is unreachable and there is no operational impact on the OT/ICS network.

The addition of security monitoring technologies to the software security program does not change the outcome - the malware is still defeated because of its inability to connect to its C2.

Adding a unidirectional gateway at the IT/OT interface also reliably defeats this attack, but for a different reason. The gateways are neither routers nor firewalls. The gateways are most often ICS clients on the OT network, and IT clients on the IT network. The gateways are incapable of sending connection attempts to the C2 on the Internet, and the gateway hardware is of course physically unable to send anything from the C2 back into the OT network.

In summary:

	Software-Based Protection	Software + Monitoring & IDS	Unidirectional Protection
Targeted OT Ransomware	✓	✓	✓

Variations: Note that straightforward variations on this attack are not so easily defeated. For example, copies of control system software packages are installed on IT computers in many industrial enterprises, to enable routine testing, development, and remote troubleshooting. If the RAT is installed on these computers on the IT network, the remote attackers will have opportunity to carry out reconnaissance on the IT network, steal credentials and eventually pivot through to the OT/ICS network where they can again, deploy their ransomware and impair operations.

#3 OT/ICS Management System Ransomware

Again, security updates are generally installed promptly on IT networks, with limited testing. The latter is because the consequences of malfunction are minimal - if security updates to management system client software prove problematic, IT teams can simply uninstall and re-install the client software on the affected machines. This means the RAT will be installed promptly on the OT/ICS management system clients, and Sunburst-class anti-virus, sandboxing and other evasions make detection of the RAT very unlikely. Software-based security systems will not defeat this class of attack.

How does this attack fare in a software-protected organization with significant security monitoring and intrusion detection capabilities? Such an organization is likely to detect the intrusion eventually - but will it be detected in time?

FireEye detected the Sunburst malware some six months after the malware was inserted into the SolarWinds security update, and FireEye is an extremely security-sophisticated target. FireEye's intrusion detection, incident response and forensic analysis capabilities are legendary in the security industry. The problem: even FireEye took months to discover the breach. Industrial enterprises focused on production rather than on security are likely to take much longer to detect such a breach, if they detect it at all.

Worse: FireEye detected the breach only after large volumes of important intellectual property had been stolen. A ransomware attack focused on sabotage would involve much smaller amounts of suspicious communications, and so would very likely take a correspondingly much longer time to detect.

In short, security monitoring, intrusion detection and incident response capabilities are important, but these are detective and reactive capabilities. These are not preventive capabilities and are unlikely to detect this attack in time to prevent physical consequences.

Unidirectionally-protected networks fare much better in the face of an attack on management servers. Unidirectionally-protected enterprises generally deploy two copies of management servers:

- One copy on the enterprise network to report OT software status to enterprise decision-makers.
- One copy on an OT WAN, to control the OT installations and report information to the enterprise system.

In these enterprises, the only connections between the OT/ICS WAN and the enterprise WAN are unidirectional, sending data from the OT network to the enterprise network.
This means that:

- Even when OT clients are compromised by a supply-chain RAT, those clients cannot receive instructions from an Internet-based C2.
- No matter what happens on the Internet-exposed enterprise network, no compromise or attack instructions from the management server or from any other part of the enterprise network can propagate back into the OT network

This two-server design for management systems provides almost all the cost savings and efficiency benefits of the single-server design, without the truly unacceptable risks that accompany Internet-exposed single points of compromise.

In summary:

	Software-Based Protection	Software + Monitoring & IDS	Unidirectional Protection
OT Management Ransomware	✗	✗	✓

#4 IIoT Ransomware

This attack happens extremely quickly and is difficult to detect. Anti-virus systems and sandboxing systems are generally not able to inspect device firmware. Whitelisting generally cannot be deployed on IIoT devices, and even if it is deployed, the malicious inclusions are marked by the software update system as legitimate updates, and so permitted by the whitelisting system to operate.

Intrusion detection and security monitoring system are very unlikely to detect this attack, either. Firmware updates are downloaded to IIoT devices routinely, and the intrusion detection system has no way of knowing that the firmware download timing is no longer under the control of the device or the site.

The unidirectional security posture, however, does defeat this attack. When a unidirectional gateway sits between IIoT devices and the Internet, there is no way for firmware updates or any other attack signals to reach IIoT devices to impair their operation. Firmware updates in unidirectionally-protected installations must be carried out via local IIoT update servers. Such updates are generally authorized and activated in those update servers only after extensive testing by the engineering team.

In summary:

	Software-Based Protection	Software + Monitoring & IDS	Unidirectional Protection
IIoT Ransomware	✗	✗	✓

Conclusion

The combination of supply chain and ransomware attacks poses a serious threat to industrial operations. Supply chain attacks are on the rise, and targeted ransomware is already the single biggest cause of production downtime due to cyber attacks. Software-based and the combination of software and detective measures are adequate to defeat only the very simplest of these attacks. More sophisticated attack teams are very much capable of defeating software-based security measures.

Unidirectional gateway technology provides robust protection from targeted ransomware and supply-chain ransomware attacks. In the representative attack scenarios we explored above:

	Software-Based Protection	Software + Monitoring & IDS	Unidirectional Protection
Ransomware Time Bomb	✗	✗	✓
Targeted OT Ransomware	✓[1]	✓[1]	✓
OT Management Ransomware	✗	✗	✓
Cloud / IIoT Ransomware	✗	✗	✓

[1] Software-based protections would not, however, protect against straightforward variations of this attack.

Unidirectional gateways enable the efficiencies of IT/OT integration and OT/cloud analytics without the serious security risks that come with firewalled IT/OT and cloud connections.

Waterfall Security Solutions

Waterfall Security Solutions is the world's leading provider of Unidirectional Security Gateway products and technologies, enabling 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.