Lessons from 2020: Defeating Targeted Ransomware Attacks at Industrial Sites

Mike Firstenberg
Director of Industrial Security
Waterfall Security Solutions

2020 was not a good year for cyber attacks on industrial control systems (ICS) and operational technology (OT) networks. Nine attacks shut down physical operations at industrial sites, and all were targeted ransomware. In addition, 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. Ransomware, targeted ransomware, supply chain breaches and the continued complexities of cloud connectivity are all 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.

Targeted Ransomware

The public reports of these nine attacks shutting down industrial processes show that 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.

Targeted ransomware in both the IT and ICS/OT space can be very sophisticated. Many of the criminal groups behind today's ransomware are using attack tools and techniques that were 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 can thus increase the likelihood of a payout to the criminals.

Target	Plant-Days Lost	Head Office
Picanol	196	Belgium
Steelcase	140	USA
Lion	63	Australia
Southwire	50	USA
X-FAB	48	Germany
Fisher & Paykel	25	New Zealand
Tower Semiconductor	18	Israel
Honda	8	Japan
BlueScope Steel	2	Australia

SolarWinds Orion / SUNBURST

The biggest cyber breach in 2020 was the SolarWinds Orion supply chain breach. Sophisticated attackers inserted multiple versions of remote control malware into security updates for the SolarWinds Orion security product. The updates beaconed out to command-and-control centers, providing the attackers with remote control of compromised equipment. Up to 18,000 sites were affected. Up to 200 were actively exploited by remote control. While many industrial operations were impacted and had to clean out the SUNBURST and other malware artifacts, there are thus far no public reports of OT / industrial downtime due to the attack. Nonetheless, this is seen by most practitioners as an unacceptably near miss.

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/OT networks. The average industrial site in process industries such as power generation and refining has up to a half dozen connections to Internet-based vendors such as equipment manufacturers and control system software manufacturers. The average discrete manufacturing site, such as computer or automobile and parts manufacturers, has many dozens of such connections, because of the much wider variety of specialized machines and robots used in discrete 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 ICS/OT networks is worsening because of very sophisticated, targeted attacks, the increase

in cloud connectivity in these same networks is increasing opportunities for supply-chain-based cyber attacks.

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 seems 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 industrial sites will only make this class of attack easier for the criminal groups involved. Enterprise and engineering security teams all over the world are taking these developments in the pervasive threat environment into account in their security planning for 2021.

What To Do?

The majority of industrial, operations and manufacturing sites rely heavily on software-based security systems. Best practice software systems can include layers of firewalls, encrypted communications, least-privilege account management, security update/patching programs, anti-virus systems, and mandatory access controls, among others. While software-based security programs can use all of such practices in principle, most do not. The omissions are generally because of cost and compatibility issues. Software-based security programs can be complex and expensive, especially security update and security monitoring programs.

As a result, a rapidly growing number industrial enterprises deploy unidirectional gateway hardware, software and related technologies to provide robust compensation for these omissions. Unidirectional gateways are simple – the hardware is physically able to send efficiency-enabling industrial information from industrial networks out to business networks, but not physically able to send any cyber attacks back into protected networks. The gateway software makes copies of servers – everything from databases and MES servers to historians and OPC servers. Enterprise users and applications access the enterprise copies normally and safely. In short, the technology provides enterprise networks with access to industrial data, without access to industrial systems.

Because of the strength of protection afforded by the technology, unidirectionally-protected sites are able to reduce their expenditures on the most complex and most costly of software security mechanisms, such as security update programs, without impairing their security posture.

Conclusion

The combination of cloud connectivity, supply chain breaches and targeted ransomware poses a serious threat to industrial operations. These classes of attack routinely defeat software-based preventive and detective measures. This is why so many industrial sites are adding a layer of unidirectional protection into their defense-in-depth security architectures. Unidirectional gateways enable the efficiencies of IT/OT integration and OT/cloud without the serious security risks and security program costs that come with increased IT/OT connectivity in classic software-only defensive postures.

Further Reading

Waterfall's latest report *OT/ICS Ransomware and the Supply Chain: Learnings from Attacks in 2020* explores all of these topics in greater detail.

About Waterfall Security Solutions

Waterfall Security Solutions is the OT security company, producing a family of Unidirectional Gateway technologies and products that enable enterprise-wide visibility for operations, with disciplined control. Waterfall products represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, utility companies, 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.

# # #