WHITE PAPER

Securing OT Systems in the Face of Rapid Threat Evolution

What CISOs with OT Need To Know About the Advanced Threat Landscape

Executive Summary

Many businesses that rely on operational technology (OT) have managed those systems in the same way for decades, including security of the OT equipment. Much of the industrial equipment in use today was developed at a time when every business maintained an "air gap" between OT and information technology (IT) systems. Now, however, OT systems are being connected to IT networks and the internet, exposing them to sophisticated advanced threats, which their security functionality may not be prepared to detect or respond to. Chief information security officers (CISOs) should be particularly concerned about attacks on OT systems because they can result in far more damage than a typical data breach or ransomware attack. On top of financial and reputational impacts, compromised OT systems may result in diminished productivity, damaged assets, and safety risks for employees and others.

94% of survey respondents in OT organizations make OT security posture a significant or moderate factor in the corporate risk score the CISO shares with executive leadership and the board.[4]

OT Organizations Under Growing Threat of Attack

As organizations modernize and embrace efficiency gains from Industrial Internet-of-Things (IIoT) technologies, the air gap between IT and OT disintegrates, and the attack surface expands. OT sensors are increasingly being integrated into IT networks to interface with machine learning and big data technologies. This connectivity creates both competitive advantage for the company and an increased risk of cyber intrusion. The growing attack opportunities are especially problematic because "headless" OT devices were not designed with security in mind. They cannot run standard security-client software, and uptime requirements often result in very narrow windows for security updates. As a result, companies may apply only the most critical patches.

Attacks on OT systems create serious risks for the organization. An intruder may not be looking to steal data, but instead may intend to stop equipment or alter its function. Whether the goal is to shut down a production line, open a valve that should stay closed, or turn off critical process monitors, such an attack can wreak havoc on the organization and its customers. Alternatively, such an attack may be intended instead to utilize IT-OT network connections for lateral movement into the company's IT systems. If OT defenses are easier to penetrate, a successful breach might give an attacker access to customers' personally identifiable information (PII) or corporate financial data.

Nearly three-quarters of OT organizations experienced at least one cyber intrusion in the past 12 months, and half experienced three or more intrusions.[1] Moreover, almost all organizations (97%) that use supervisory control and data acquisition (SCADA) or industrial control system (ICS) technologies acknowledge the security challenges created by the convergence of IT and OT.[2] Some of the attacks on OT involve repurposed malware; once IT security solutions are effectively blocking a threat, creators of the malware may try to use it against OT systems with less sophisticated protections.[3] However, an increasing proportion of attacks on OT systems are built specifically to penetrate the defenses of operational equipment.

Evolution in the Advanced Threat Landscape

Purpose-built OT attacks are designed to target the weakest points of OT networks, which are generally the smallest and simplest portions of the infrastructure. Bridges and serial converters are a common focus.[5] Industroyer, a malware attack that brought down Ukraine's power grid in 2016, attacked protection relays.

The attack was multipronged, but it started by exploiting a known vulnerability in digital substation relays produced by Siemens.[6] The malware used this vulnerability to access the network of OT devices supporting Kiev's power grid. It created two backdoor network access points, then simultaneously deployed on all the circuit breakers and protection relays that it could reach, as well as on the Windows workstations that ran ABB MicroSCADA software to control those devices.

The attack was regulated by a timer. When the appointed time arrived, it performed a distributed denial-of-service (DDoS) attack on every protection relay on the network that used any of four communication protocols.[7] At the same time, it deleted all MicroSCADA-related files from the workstations' hard drives. The immediate result of this sophisticated attack was unresponsiveness of relays across the network, which caused a power outage for all of Kiev. The damage did not stop there. Years later, Industroyer continued to attack OT devices around the world.[8]

While Industroyer was an early example, the trend toward increasing OT-specific attacks continues. Today, 85% of all OT threats target one of three OT control protocols.[9] One is OPC Classic, which was developed in the 1990s and 2000s. Systems using this protocol are attractive to attackers because they are so prevalent; it is the most-used OT protocol. Second is BACnet, which dates back to 1987 and is used by many heating, ventilation, and air conditioning (HVAC) systems, including those made by Johnson Controls and Carrier. In 2018, the top three threats in terms of number of devices using them were all on the BACnet protocol.[10] The third is Modbus, an OT communication protocol that was developed in 1979. Four decades ago, developers expected that systems would always be air gapped. Another challenge for those responsible for OT security is that Modbus has numerous iterations, created by an assortment of vendors. Tracking known Modbus vulnerabilities is time-intensive.[11]

Another challenge for OT security managers is that targeted attacks are often designed to focus on systems that are under peak load, when attacks can do the most damage or create maximum pressure on the victim organization to comply with the perpetrator's demands. For example, attacks on HVAC systems and electrical grids in North America spike during summer months.[12]

"Complex malware like Industroyer typically enjoys a long life, even after detections and signatures have been deployed."[13]

"Attackers have moved from spreading malware [with the intent] to cause widespread havoc across multiple systems, to gaining detailed knowledge on industrial control systems to target specific industries, countries, and companies."[17]
– Mark Carrigan, Chief Operating Officer, PAS Global

Increasingly sophisticated threats are harder to detect

No vendor of SCADA or other ICS systems is immune to these risks. A 2019 Fortinet study of OT threats found that although Advantech, Schneider Electric, Moxa, and Siemens devices were most frequently attacked, every one of the 70 vendors evaluated faced ongoing attacks on a regular basis.[14] Moreover, the study showed that the number and rate of attacks are increasing for almost every SCADA and ICS vendor.

These attacks are becoming increasingly targeted. They focus on a specific desired result at a single organization, then take a multipronged approach to achieving that goal. Industroyer is a case in point. The attack was executed over the course of months, with a specific deployment date. (Russia is believed to have perpetrated Industroyer for the purpose of hobbling Kiev in support of the precisely timed Russian invasion of Ukraine.) Moreover, the attack involved several discrete steps: entry into the OT network via the Siemens relays, creation of two separate backdoor access points, deployment on OT devices and computer workstations networkwide, then activation.

Attacks on OT systems are also becoming increasingly evasive. Their malware often includes functionality specifically designed to evade antivirus or threat-detection solutions. Malware may be able to detect when it is running in a sandbox environment, it may be capable of disabling security tools on infected machines, and it may use junk data to make disassembly harder.[15] More and more OT-targeting malware employs encryption to avoid detection, and security researchers have discovered highly sophisticated evasion tactics such as the Ryuk ransomware's ability to destroy its own encryption key and delete shadow copies from infected systems.[16]

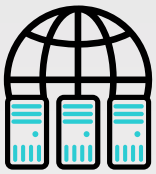
Attacks on Triconex systems go unnoticed for months

The TRITON attack, also known as TRISIS, targets Triconex safety instrumented system (SIS) controllers developed by Schneider Electric. TRITON's first known exploit attacked a Saudi Arabian petrochemical plant. The malware gained access to the company's IT network through means that are unknown but suspected to have been a phishing attack.[18] Once inside the IT perimeter, the attackers moved laterally into the OT side of the organization. Although the plant had deployed a "demilitarized zone" (DMZ) architecture in which IT and OT networks were separated by a firewall, the attackers initiated Remote Desktop Protocol (RDP) sessions to the plant's engineering workstations from within the IT network.[19]

The first known incident to attack an OT engineering department,[20] TRITON/TRISIS seems to have focused on network reconnaissance. The attackers did not steal data, take screenshots, or log keystrokes.[21] Instead, they harvested user credentials through malware that created backdoors in both the IT and OT networks, then used those backdoors to gain access to the SIS engineering workstations. The malware also renamed its own files to look like Microsoft Update files and used both webshells and secure shell (SSH) tunnels.[22]

The attackers gained access to the plant's distributed control system (DCS), but they seem to have been focused solely on the SIS controllers.[23] Ultimately, their sophistication was for naught; the six infected Triconex SIS systems shut down in what seems to have been an accidental trigger of the malware ahead of the attackers' planned schedule.[24] They entered a "failed safe" state, and disaster was averted.[25]

Nevertheless, the attack reveals the degree to which a committed coder may develop a multifaceted attack that uses highly sophisticated methods (e.g., changing filenames, developing and deploying SSH tunnels, creating multiple backdoors for network access) to bypass standard security measures. In fact, the malware was so elusive that the attackers' first attempt—a shutdown two months earlier of a single Triconex SIS system at the same plant—went undetected. Schneider Electric pulled log files from the device, ran diagnostics on the data it collected, and identified the problem as a mechanical issue.[26]



"The plant on paper had a secure architecture. But we identified a poorly configured DMZ infrastructure that allowed the attackers to compromise the DMZ and pivot to control the network."[27] – Julian Gutmanis, Principal Threat Analyst, Dragos Inc.

"[The] threat landscape should be taken seriously by any organization that has connected ICS/SCADA systems. Adversaries are thinking strategically, extracting as much value as possible from each new threat they develop by exploiting unprotected systems and vulnerabilities."[33]

Unknown and zero-day exploits are often ignored

Known malware can be difficult to detect when its sophistication reaches that of the TRITON/TRISIS attack. In fact, TRITON/TRISIS compromised a second victim in the Middle East in April 2019,[28] and the group thought to be behind TRITON/TRISIS reportedly attacked several North American oil-and-gas targets in early 2019 as well.[29]

However, successful known malware is not the only risk to OT systems. New and innovative attacks are surfacing continuously. One example is LockerGoga, a ransomware scheme that temporarily stopped production in Norsk Hydro aluminum plants around the world in March 2019. That attack's key innovation was that it distributed the malware without using network traffic, Domain Name System (DNS), or command-and-control servers.[30] Instead, it spread the malware using the network's own Active Directory services.[31] On the day after LockerGoga was first detected at Norsk Hydro, only 17 out of the top 67 antivirus products recognized it as a threat.[32]

OT Breaches Cause Heavy and Sustained Losses

The business impact of OT breaches can be severe. Some, like LockerGoga, are designed to disrupt OT systems in hopes of receiving a payout. However, many are designed to shut down or damage industrial equipment.[34] Unexpected stoppage of a production line obviously damages the company's ability to meet production targets, perhaps for an extended period of time.

Any downtime in OT systems can result in immediate loss in revenue, which can add up to hundreds of thousands or even millions of dollars in just minutes, depending on the company. For example, NotPetya ransomware in 2017 cost pharmaceutical giant Merck nearly $1 billion when it shut down production.[35] At shipping giant Maersk, NotPetya caused a 20% drop in volume, costing $300 million.[36] Many companies were still wrestling with the consequences of NotPetya a year later.[37]

In an OT attack, environmental damage is a real possibility as well. Although this ultimately did not happen, the TRITON/TRISIS attack had the potential to cause toxic hydrogen sulfide gases to be released into the atmosphere.[38] Such an environmental failure would likely result in cleanup costs and regulatory penalties, and might also have a serious impact on the company's brand reputation.

Moreover, when OT equipment stops unexpectedly, it creates risk of injury or even death for the employees operating the equipment. In medical environments, these risks extend to patients, whose health could be jeopardized if a machine such as a ventilator stopped without warning. Hospital security teams are becoming increasingly concerned about the potential for attacks seeking to disrupt hospital operations in this way.[39]

Research into cyberattacks at OT organizations reveal all of these effects. More than one in four respondents (43%) in a recent Fortinet study said the operational outages they experienced had impacted productivity, while 36% said outages had impacted revenue, 23% said they put physical safety at risk, 30% said they resulted in degradation of brand awareness, and 28% said the OT attack led to the loss of business-critical data.[40]

NotPetya ransomware cost Merck nearly $1 billion and cost Maersk $300 million.[41,42]

Conclusion: Weighing the Risks

The costs of an OT attack are far too high to ignore. CISOs in industries that rely on operational and industrial production systems—such as manufacturing, utilities, and transportation—are under increasing pressure to ensure the operational side of their network is adequately protected. However, traditional approaches to OT security cannot keep pace with the rate of evolution of advanced threats.

Considering the potential severity of a breach's consequences, CISOs should ask themselves several questions:

- Am I confident in the ability of our vendors to detect attacks on all our business-critical OT systems?
- Does our organization have the ability to identify unknown and zero-day threats?
- Do we have the right processes in place to mitigate any risks that are uncovered?
- Do our systems include incident-response technologies that can thwart advanced security threats that use obfuscation?
- What are the potential impacts of a breach? If I need to build a business case for improving OT security, which risks stand out as most critical to address?

The CISO who can confidently answer these questions is better positioned to protect the OT systems that are fundamental to the organization's operations.

[1] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[2] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

[3] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 16, 2019.

[4] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[5] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 16, 2019.

[6] Charlie Osborne, "Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout," ZDNet, April 30, 2018.

[7] Ibid.

[8] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems,"" Fortinet, May 16, 2019.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] "Threat Landscape Report Q2 2019," Fortinet, Q2 2019.

[16] Ibid.

[17] Robert Lemos, "TRITON Attacks Underscore Need for Better Defenses," Dark Reading, April 15, 2019.

[18] Thomas Roccia, "Triton Malware Spearheads Latest Generation of Attacks on Industrial Systems," McAfee, November 8, 2018.

[19] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known," Dark Reading, January 16, 2019.

[20] Ibid.

[21] Charlie Osborne, "Triton hackers return with new, covert industrial attack," ZDNet, April 10, 2019.

[22] Ibid.

[23] Ibid.

[24] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known," Dark Reading, January 16, 2019.

[25] Charlie Osborne, "Triton hackers return with new, covert industrial attack," ZDNet, April 10, 2019.

[26] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known," Dark Reading, January 16, 2019.

[27] Ibid.

[28] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 16, 2019.

[29] "Threat Landscape Report Q2 2019," Fortinet, Q2 2019.

[30] Dan Goodin, "'Severe' ransomware attack cripples big aluminum producer," Ars Technica, March 19, 2019.

[31] Mathew J. Schwartz, "Hydro Hit by LockerGoga Ransomware via Active Directory," BankInfoSecurity, March 20, 2019.

[32] Dan Goodin, "'Severe' ransomware attack cripples big aluminum producer," Ars Technica, March 19, 2019.

[33] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 16, 2019.

[34] Robert Lemos, "TRITON Attacks Underscore Need for Better Defenses," Dark Reading, April 15, 2019.

[35] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 16, 2019.

[36] Iain Thomson, "NotPetya ransomware attack cost us $300m," The Register, August 16, 2017.

[37] Kim S. Nash, et al., "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs," The Wall Street Journal, June 27, 2018.

[38] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known," Dark Reading, January 16, 2019.

[39] Mark Klimek, "Hospitals face rising risk of sophisticated cyberattacks," Healthcare Finance, September 17, 2019.

[40] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[41] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 16, 2019.

[42] Iain Thomson, "NotPetya ransomware attack cost us $300m," The Register, August 16, 2017.

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 24, 2021 8:41 PM

wp-FA-securing-ot-systems-in-the-face-of-rapid-threat-evolution-370120

370120-A-0-EN