WHITE PAPER

The Destructive and Costly Growth of the OT Threat Landscape

Vulnerabilities in OT Systems Are Under Attack

Executive Summary

Operational technology (OT) network operations analysts face an advanced threat landscape. Both traditional attacks and more sophisticated exploits are becoming much more prevalent. Bad actors are focused on industrial targets due to the inherent vulnerabilities in legacy systems as well as the increase of information technology (IT) network connections in the OT environment.

When OT industrial equipment systems are connected to IT networks, the OT network is exposed to more attacks because the "air gap" that protected it no longer exists. Malware and other types of cyberattacks are increasing in frequency and potency and now are not only threatening to disrupt businesses but also impacting the safety and security of OT systems as well.

Indicators of threats were observed in more than 1 out of 5 sites (22%). Suspicious activities such as port scanning, malicious DNS queries, abnormal headers, and excessive number of connections between devices are flagged as indicators of threats.[1]

Cyberattacks Are Getting More Sophisticated and Extensive

Despite investments in cybersecurity technology within their organization and policies to protect industrial control systems (ICS), network operations analysts are seeing more sophisticated attacks in their OT environments. Bad actors are going full throttle with these threats, developing and deploying highly complex attacks faster than network operations analysts can respond. Successful exploits now involve sabotaging and disrupting industrial environments such as oil and gas refineries, power plants, and heavy manufacturing, among others.

Although proven attack methods such as phishing, distributed denial-of-service (DDoS), and credential compromises remain successful and are even still evolving, new threats continue to emerge. Attackers are thinking strategically and extracting as much value as possible from every new attack. So it is not surprising that 9 out of 10 OT organizations reported at least one breach in the past year that resulted in data loss, operational disruptions or outages, and/or brand degradation.[2]

OT systems need to be highly available and resilient as well as secure, and network operations analysts have reason to be concerned about these advanced threats, especially since many supervisory control and data acquisition (SCADA) and ICS systems and devices are now connected to IT networks.

Compounding the problem is the constant introduction of new applications and software capabilities to the enterprise, which increases the number of connections and overall risk exposure. The introduction of 5G and Industrial Internet of Things (IIoT) only exacerbates the problem of the increased attack surface.

Exploring OT Attack Vectors and New Vulnerabilities

For OT, the leading forms of intrusion are malware (57%) and phishing (58%).[3] When it comes to malware, cyber criminals now use automation to monitor and target specific vulnerabilities, while implementing a wide variety of exploits that can be automatically updated at any time. And with many OT environments lagging in security best practices, bad actors are reaping the rewards by recycling existing malware to exploit OT vulnerabilities. Following are some of the attack vectors cyber criminals currently employ when targeting OT environments:

Lateral reconnaissance and attack

Upon successful entry to a network, attackers search for new vulnerabilities. This tactic is particularly effective with newly connected OT systems. In the reconnaissance phase, attackers test a wide variety of older malware on a smaller number of machines. Once they are in, they go into attack phase using previously successful exploits to target other machines on the network. Remote access enables them to move laterally (east-west) from IT to OT networks, silently and stealthily expanding their presence in the environment.

Remote Desktop Protocol (RDP)

Remote Desktop Protocol (RDP) is one of the more popular ransomware exploits. Introduced in 1996, every Microsoft Windows system since Windows XP uses RDP for remote connections. Cyber criminals hack into machines using this protocol, and use RDP attacks to deploy ransomware and lock up systems. An RDP attack on Labcorp (Laboratory Corp. of America) deployed ransomware on thousands of PCs and almost 2,000 servers of this medical testing facility.[4]

Weakest protocol links

Another successful tactic used by cyber criminals is to target the weakest links in each protocol. Within the network, structural problems are exacerbated by the lack of standard protections and lack of security hygiene practiced in many OT environments. These poor security practices are a legacy of the years when OT systems were air gapped.

By far, the most targeted protocol in terms of traffic is OPC Classic, which is the predecessor of OPC UA but far more widely adopted. OPC Classic uses legacy technology, with most of it developed in the late 1990s and 2000s. But the prevalence of these systems and the siloed manner with which the elements were developed make it a tempting target for bad actors.

Ransomware has grown a staggering more than tenfold over the past 12 months. Several of the top sectors are operational technology industries, from automotive and manufacturing to energy and transportation.[5]

BACnet is the second most attacked protocol, followed by Modbus, a communications protocol that helps different components of OT systems interact effectively. Modbus is particularly difficult for OT teams to identify, track, and remediate, as it has dozens of different iterations created by different vendors.

Industrial Attacks Increase in Frequency and Devastation

In recent years, there have been a shocking number of attacks on critical infrastructure around the world, as well as many close calls. These examples are just a few of the exploits that network operations analysts face in today's risk-laden OT environment.

Cyberattacks and vulnerabilities exploited in the OT infrastructure

Threats targeting OT systems are on the rise. The current lack of effective OT security contributes to these risks. SolarWinds is a U.S. information technology firm that was the victim of a cyberattack that spread to 33,000 of their customers and went undetected for months. When SolarWinds sent out software updates to its customers, it included hacked code that created a backdoor to the customer's information technology systems, which the attackers used to install more malware, so they could spy on companies and organizations.[6]

Colonial Pipeline is one of the largest oil pipelines in the U.S. The company was the victim of a ransomware attack in May 2021 that infected some of its digital systems. Colonial Pipeline shut down more than 5,500 miles of pipeline for several days to prevent the ransomware from spreading.[7]

A hacker was able to remotely gain access to a water treatment plant near Tampa, Florida, in an unsuccessful attempt at what could have amounted to a mass poisoning. The hacker briefly increased the amount of sodium hydroxide (lye) from 100 parts per million to 11,100 parts per million at the treatment plant, which provides water to businesses and about 15,000 residents.[8]

Malware-as-a-Service

Two significant ransomware families—Sodinokibi and Nemty—were deployed as a Malware-as-a-service (MaaS) offering. Sodinokibi is malware that is constantly evolving and employing tactics that comprise remote management software consoles to infect systems. Similarly, Emotet, a popular and successful banking Trojan, launched a similar service by renting access to devices infected with the Emotet Trojan so attackers can infect those devices with additional malware such as the TrickBot Trojan and Ryuk ransomware.

DDoS attacks

A Utah-based renewable energy company that has wind and solar power generation assets across three states fell victim to a DDoS attack that briefly brought down communications to those sites. The attack left operators at the company unable to communicate with a dozen generation sites for five-minute intervals over the course of several hours. This attack is believed to be the first cybersecurity incident on record that caused a disruption in the U.S. power industry, as defined by the U.S. Department of Energy.[9]

Traditional Defense Cannot Keep Up With Advances in Threats

Cyber criminals are developing and implementing automated and scripted exploits to drastically increase the speed and scale of their attacks. Making this possible are the growing number of Internet-of-Things (IoT) and OT devices in network infrastructures. Network operations analysts struggle to combat these advanced threats due to the older technology and less developed security operations of their OT systems. It is a fact that OT has not solved some of the security issues that IT has resolved and struggles with lateral (east-west) movement of intrusions.

The increasing use of artificial intelligence (AI) in OT environments has the potential improve security, but is also likely to lead to an increase in AI-driven attacks. As advanced capabilities like AI continue to enter networks, their adoption and use by cyber criminals will only make attacks more difficult to combat.

IoT devices are also a major contributor to the increased attacks on OT. One of the primary reasons is due to the number of sensors and devices being connected to an organization's ICS. On the positive side, these new technologies introduce opportunities to improve efficiency, productivity, production flexibility, operational uptime, and visibility. But this digital innovation also greatly increases the number of attacks because there are many more IP-based devices and interfaces for cyber criminals to infiltrate.

There were 5.4 million recorded DDoS attacks during the first half of 2021—a figure that represents an 11% rise compared with the same period last year.[10]

RDP attacks skyrocketed due to the move to remote work. Between Q1 and Q4 2020, RDP attacks grew 768%.[11]

As More Threats Emerge, Consequences for OT Become More Severe

Network operations analysts for OT stand at a critical intersection between business and societal consequences. Many attacks within the IT network target data theft. But with OT, current and future breaches can compromise entire control systems that operate critical infrastructure.

Nation-state attacks on critical infrastructures such as power stations and electrical grids are cause for alarm. The number of key nation-state attacks has risen significantly over the past three years and enterprises and businesses are increasingly being targeted. State-linked groups are also finding new uses for IoT botnets, such as Tor-like communication infrastructure.[12]

Successfully executed attacks on systems like power plants, natural gas pipelines, or nuclear facilities could have cataclysmic ramifications. Disruptions might include prolonged blackouts, disrupted transportation systems, and even limited supply of fresh water.

Without electrical power, there is no internet, banking, or communications. Without reliable power, devices can't operate and internet services go down. When a cyclone hit Bangladesh last year, networks were disrupted when 60% of towers in the south of the country were cut off from power supplies.[13] Cyber threats pose a growing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices.

Conclusion

As new digital technologies explode across organizations and industries, cyber criminals are simultaneously expanding their capabilities, leveraging new techniques, and integrating into systems—sometimes waiting silently in a network for months, even years, before attacking.

As the threat landscape increases in volume and velocity and becomes more sophisticated, malicious groups apply best practices to extend the reach of attacks, using advanced software that propagates multivector attacks, use AI and machine learning to probe for vulnerabilities and exploit them before they can be patched, release terabit-per-second DDoS attacks, and much more.

With the air gap no longer a barrier between bad actors and OT environments, network operations analysts must be aware of these advanced threats and ensure that they have the right security technologies and best practices in place to combat them.

[1] "2020 Global IoT/ICS Risk Report," CyberX, 2020.

[2] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[3] Ibid.

[4] Brian Pereira, "What is an RDP attack?" CISOMAG, January 14, 2021.

[5] Derek Manky, "Critical Cyber Threat Landscape Insights from 2021 for CISOs," Fortinet, September 7, 2021.

[6] Isabella Jibilian and Katie Canales, "SolarWinds Hack Explained," Business Insider, April 15, 2021.

[7] Sean Michael Kerner, "Colonial Pipeline hack explained: Everything you need to know," TechTarget, July 7, 2021.

[8] "Hacker attempted to poison water supply of Florida city, officials say," The Guardian, February 8, 2021.

[9] "Details of Attack on Electric Utility Emerge," Dark Reading, November 2, 2019.

[10] Danny Palmer, "DDoS attacks are becoming more prolific and more powerful, warn cybersecurity researchers," ZDNet, September 22,2021.

[11] Kelly Sheridan, "RDP Attacks Persist Near Record Levels in 2021," Dark Reading, March 17, 2021.

[12] Danny Palmer, "Nation-state cyberattacks targeting businesses are on the rise," ZDNet, April 9, 2021.

[13] Anju Mangal and Nathalia Foditsch, "No connectivity without electricity: how a lack of power keeps millions offline," Alliance for Affordable Internet, March 10, 2021.

November 2, 2021 7:36 AM

501171-A-0-EN