The Destructive and Costly Growth of the OT Threat Landscape

Vulnerabilities in OT Systems Are Under Attack
Executive Summary

The network operations analyst for operational technology (OT) faces an advanced threat landscape, with both traditional attacks and more sophisticated exploits becoming much more prevalent. Bad actors are focused on industrial targets due to inherent vulnerabilities in legacy systems, as well as the increase of information technology (IT) connections in the OT environment. When industrial equipment is connected to IT networks, systems become exposed to more attacks since the “air gap” that was originally designed to protect only the perimeter no longer exists. As a result, malware and other types of cyberattacks are increasing in frequency and potency, not only threatening to disrupt businesses but also impacting the safety and security of the systems on which OT organizations depend.

Introduction: 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.

While proven attack methods—phishing, distributed denial-of-service (DDoS), and credential compromise—remain successful and are even still evolving, new threats continue to emerge. Attackers seem to be always a step ahead, thinking strategically, extracting as much value as possible from every new attack. For those reasons, it is unsurprising that nearly three-quarters of 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

Charged with designing and building OT systems that are highly available and resilient as well as secure, 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 their 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 in doing so, overall risk exposure as well.

Exploring OT Attack Vectors and New Vulnerabilities

For OT, malware is the leading form of intrusion (77%), followed by phishing (45%), spyware (38%), and mobile security breaches (28%).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

One tactic attackers take upon successful entry to a network is to cast about for new vulnerabilities; this is particularly effective with newly connected OT systems. In the “reconnaissance” phase, they 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 many 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)

One of the more popular ransomware exploits is RDP. This works when attackers gain access by stealing remote access credentials through phishing attacks, social engineering, brute-force attacks, or by simply sniffing plaintext passwords. As an example, security researchers recently discovered a new botnet that attacked millions of Windows systems running an RDP connection exposed to the internet.

Weakest protocol links

Cyber criminals find targeting the weakest links in each protocol a successful tactic as well. Within the network, structural problems are exacerbated by the lack of standard protections and poor security hygiene practiced in many OT environments—a legacy of the years when they were air gapped. By far, the most targeted protocol in terms of traffic is OPC Classic, the predecessor of OPC UA but currently far more widely adopted. This protocol uses newer 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 makes it a tempting target for bad actors.

BAConet 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. Following are just a few specific exploits that network operations analysts face in today’s risk-laden OT environment:

Cyberattacks with exotic names

Recent OT-specific exploits include Stuxnet, Havex, Industroyer, and TRITON/TRISIS. Industroyer and Havex are thought to have been used by Russian forces as cyber weapons targeting Ukraine’s power grid in 2016. The malware has since leaked and been reutilized against various other grids where the same Schneider Electric infrastructure is found.

Vulnerabilities exploited in the OT infrastructure

In late 2019, many vulnerabilities were disclosed in Wind River VxWorks, a trusted real-time operating system (RTOS) deployed on more than 2 billion embedded devices. Vulnerabilities in these devices gave attackers a way to steal data, execute DDoS attacks, and perform other malicious actions. Over 200 million devices were affected, including mission-critical SCADA and other devices running in industrial settings. It also impacted enterprise firewalls and printers as well as healthcare systems such as patient monitoring devices and MRI machines.

Malware-as-a-Service (MaaS)

Recently, two significant ransomware families—Sodinokibi and Nemty—were deployed as a 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.
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.

Meanwhile, bad actors are laying the groundwork to adopt artificial intelligence (AI) to automatically map networks, assess vulnerabilities, choose attack vectors, and conduct penetration testing in order to deploy fully customized and automated attacks. As advanced capabilities like these continue to enter networks, their adoption and use by cyber criminals will only make it more difficult for them to combat attacks.

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.

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.

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—just chaos and disruption. In the U.S., national intelligence officials indicate 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.

Also sounding an alarm around the world are the attacks of nation-states on critical infrastructures such as power stations and electrical grids. Russia, China, North Korea, and Iran are all known to have dedicated cyber arsenals, and despite warnings, are showing no sign of slowing down their cyber activities. State-linked groups are also finding new uses for IoT botnets, such as Tor-like communication infrastructure.

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.


5. Catalin Cimpanu, “A botnet is brute-forcing over 1.5 million RDP servers all over the world,” ZDNet, June 6, 2019.


11. Sean Lyngaas, “Utah renewables company was hit by rare cyberattack in March,” CyberScoop, October 31, 2019.


19. Beatrice Christofaro, “Cyberattacks are the newest frontier of war and can strike harder than a natural disaster. Here’s why the US could struggle to cope if it got hit,” Business Insider, May 23, 2019.