FORTINET

REPORT

Fortinet 2019 Operational Technology Security Trends Report

An Update on the Threat Landscape for ICS and SCADA Systems

Table of Contents

Executive Summary

As organizations make their operations more agile in response to a quickly evolving marketplace, many operational technology (OT) systems are being connected to the outside world for the first time. This trend promises great benefits for organizations, but also exposes OT systems to advanced persistent threats. The "air gap" that protected OT systems from hackers and malware no longer exists at many organizations, and adversaries are increasingly targeting OT systems as a result.

Fortinet's 2019 OT Security Trends Report analyzes aggregate data from FortiGuard Labs to glean insights about the state of security for supervisory control and data acquisition (SCADA) and other industrial control systems (ICS). The analysis finds that OT systems are increasingly targeted by information technology (IT)-based attacks—often legacy ones that no longer affect IT systems—as well as purpose-built OT attacks. Logically, these attacks tend to be targeted at the weakest parts of OT networks and take advantage of the complexities caused by a lack of standardization of protocols. And threat actors do not discriminate according to industry or geography, as every vertical and region saw significant attacks.

As OT systems become more connected, the trend of increased attacks seems likely to continue. This new exposure requires organizations to adhere to more rigorous security operations and life-cycle management best practices to protect their organizations from major threats to the core of their business. As a result, OT and IT teams need to come together to respond comprehensively to an increasing threat.

Infographic: Key Findings

Exploits **increased in volume and prevalence** in 2018 for almost every ICS/SCADA vendor.

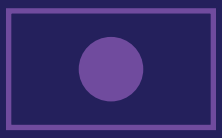
Adversaries regularly **recycle IT threats** to target OT systems.

85%

of unique threats detected target machines running:

OPC Classic
BACnet
Modbus

BACnet attacks peaked in **January-April 2018**, corresponding with the Mirai botnet.



The **Moxa 313** vulnerability was heavily concentrated in Japan.

Introduction

Historically isolated by "air gapping," OT systems are now increasingly connected—sometimes to a greater extent than plant managers and industrial control engineers realize. According to one recent study, nearly two-thirds of OT devices are connected—32% directly to the internet, and another 32% through a gateway into the enterprise.[1] This gateway is sometimes as innocuous as a single PC that is separately connected both to the OT system and the internet.

Integrating IT and OT systems is a good business decision for many organizations, with benefits that include:

- **More effective and efficient monitoring of processes**, with the ability to make important changes on the fly
- **The ability to use data from Internet-of-Things (IoT) devices** to inform decision-making, adding a very granular layer of insight about customers, products, and processes
- **Access to real-time market data** for optimal timing of product delivery and smoother interaction with the supply chain
- **Significant cost savings** in power consumption, reduced raw materials waste, and employee efficiency

Integrated OT raises security issues.

Despite these clear benefits, the elimination of the air gap exposes OT systems to the same security risks that impact IT systems—and makes OT-specific exploits easier to propagate. Compounding the problem, ICS and SCADA systems have historically operated on a much longer update and replacement cycle than IT systems, meaning that many very old technology systems are now being exposed to today's advanced persistent threats for the first time. Another challenge is a lack of visibility: 82% of respondents to one survey acknowledged that they are unable to identify all the devices connected to their OT and IT networks.[2]

At many organizations, these challenges have resulted in an unacceptably high rate of security incidents. In a recent survey of OT leaders, 77% of respondents said they had experienced a malware intrusion in the past year, and half experienced between three and 10.[3] The nature of these intrusions is concerning: respondents report events that impacted productivity (43%), revenue (36%), brand awareness (30%), data loss (28%), and even physical safety (23%).

OT security involves significant risk.

Indeed, adversaries have many incentives to attack ICS and SCADA systems. Criminals can demand a ransom after halting operations at a factory, disabling a badge access system, or taking control of a piece of critical infrastructure. Competitors—often nation-state actors on behalf of state-owned enterprises—can infiltrate systems for the purpose of industrial espionage. And attackers with political aims can target organizations perceived to stand in the way of their objectives by sowing chaos and disruption.

Those responsible for the security of OT systems face significant challenges as they go online:

- An **expanded attack surface** due to the elimination of the "air gap"
- **Legacy systems** whose security features were designed for a disconnected infrastructure
- **Poor visibility** into systems, often with IoT devices connected in a piecemeal fashion
- **Legacy telemetry devices** whose manipulation could be catastrophic
- **Poor network segmentation**, with 45% of ICS/SCADA users not making use of privileged identity management[4]

The Fortinet 2019 Operational Technology Security Trends Report analyzes data gathered from millions of Fortinet devices to discern the state of cybersecurity for ICS and SCADA systems. The resulting insights can help those responsible for securing these systems understand the risks and prioritize their responses.

OT Threat Landscape Trends

Trend: IT-Based Attacks Are Increasingly Impacting OT Systems

As OT systems are connected to IT networks, they often represent the weakest link in the security chain. Data from FortiGuard Labs indicates that adversaries are using IT-based threats to attack OT systems. Under one typical scenario, threat actors target IT and OT systems at an organization simultaneously with the same malware. Since OT systems often use older technology and security operations are frequently less developed, the attackers have a higher rate of success there.

Threat actors "recycle" malware for OT.

Another scenario involves adversaries reusing legacy malware packages that were used in the past for IT attacks, but are now caught by any signature-based IT security solution. Figure 1 shows the percentage of existing threats detected by Fortinet during each month of the year, as well as the number of devices with OT protocols hit by any of the threats each month. Note that the pattern is very cyclical: when more threats are being used, fewer devices are hit, and vice versa.

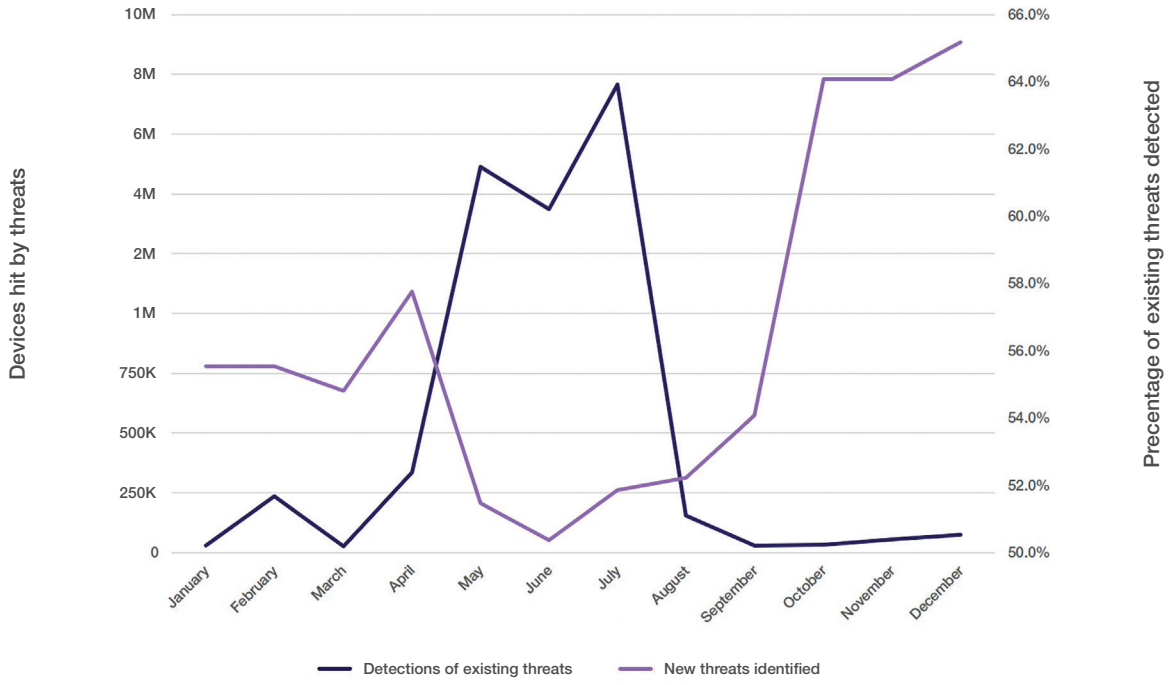


Figure 1: Percentage of existing threats detected and devices hit, 2018.

This cycle suggests that adversaries are casting about for new vulnerabilities in newly connected OT systems. In the "reconnaissance" phase, they test a wider variety of old malware on a relatively small number of machines. Once they identify the threats that were successful, they move into an "attack" phase, using the subset of attacks that proved successful on a larger number of machines. Their aim is to maximize the value of existing malware before investing in creating new, more targeted attacks.

Another factor may also contribute to this seasonal variation in the use of new versus old threats. Specifically, attacks on heating, ventilation, and air conditioning (HVAC) systems and electrical grids are more likely to occur when these systems are operating at peak usage—most often during the Northern Hemisphere's summer months. The age of an OT system is also a factor, with adversaries tending to target older technology more frequently than newer, more secure technology.

Threat actors target devices using a variety of OT protocols.

While IT systems have been standardized for many years on the TCP/IP protocol, OT systems use a wide array of protocols, many of which are specific to functions, industries, and geographies. The OPC Foundation was established in the 1990s as an attempt to move the industry toward protocol standardization. OPC's new Unified Architecture (OPC UA) has the potential to unite protocols for all industrial systems, but that consolidation is many years away due to the prevalence of legacy protocols and the slow replacement cycle for OT systems.

Cyber criminals have actively attempted to capitalize on this confusion by targeting the weak links in each protocol. These structural problems are exacerbated by the lack of standard protections and poor security hygiene practiced with many OT systems—a legacy of the years when they were air gapped. Figure 2 shows the number of unique threats targeting machines using specific ICS/SCADA protocols.

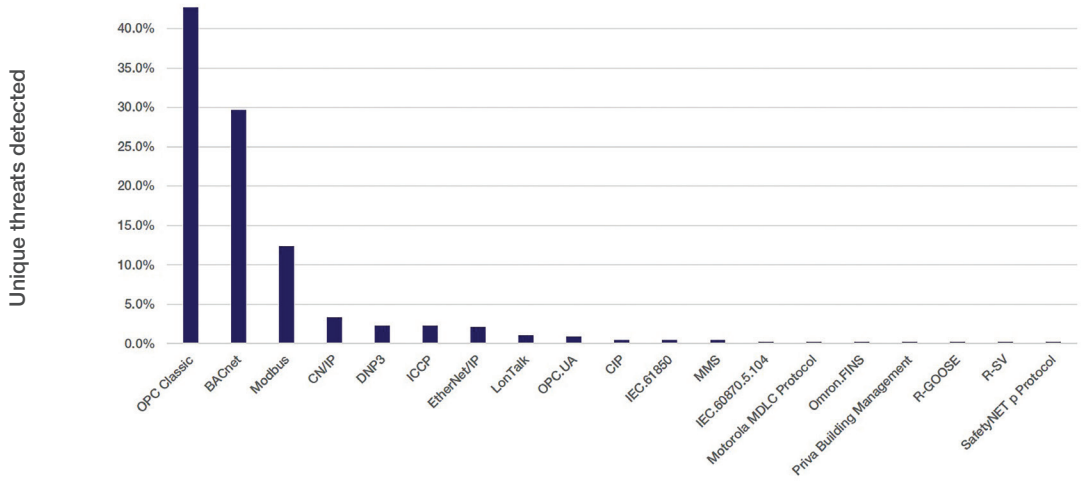


Figure 2: Number of unique threats detected targeting ICS/SCADA protocols.

Three protocols dominate in unique threats detected.

Two factors seem to govern which protocols are most targeted: how commonly they are used and how vulnerable the protocols are. Together, the OPC Classic, BACnet, and Modbus protocols account for 85% of unique threats detected on machines running OT protocols.

By far, the most targeted protocol group is **OPC Classic**, the predecessor of OPC UA but currently far more widely adopted. This protocol uses newer technology than some—most of it was developed in the late 1990s and 2000s—but the prevalence of these systems and the siloed manner with which the various elements were developed makes it a tempting target for cyber criminals.

Building automation is one area of OT that has mostly standardized on a single protocol. **BACnet** is in use at almost every sizable organization regardless of industry—partly because it is used by large HVAC vendors like Johnson Controls and Carrier. As a result, BACnet is the second most targeted protocol. Another factor: BACnet is based on very old technology going back to 1987. Three of the top four threats in 2018 in terms of number of devices they hit target users of BACnet (Figure 3). The volume of detections of attacks on BACnet machines spiked in the first half of the year (Figure 4), which corresponds with the Mirai botnet that targeted BACnet systems, causing distributed denial-of-service (DDoS) events around the world.[5]

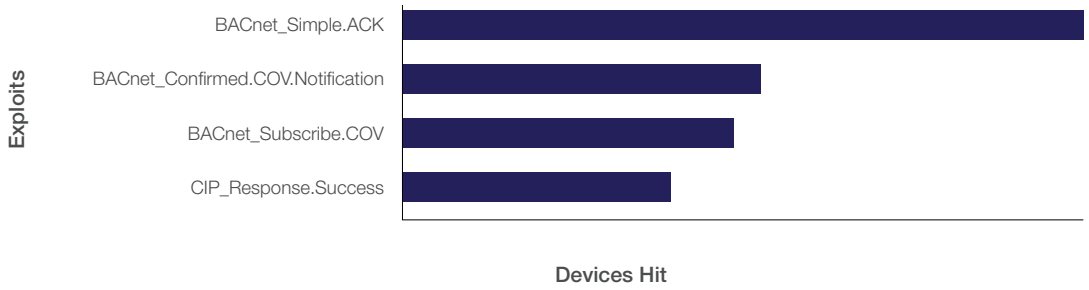


Figure 3: Top 4 exploits detected by number of devices, 2018.

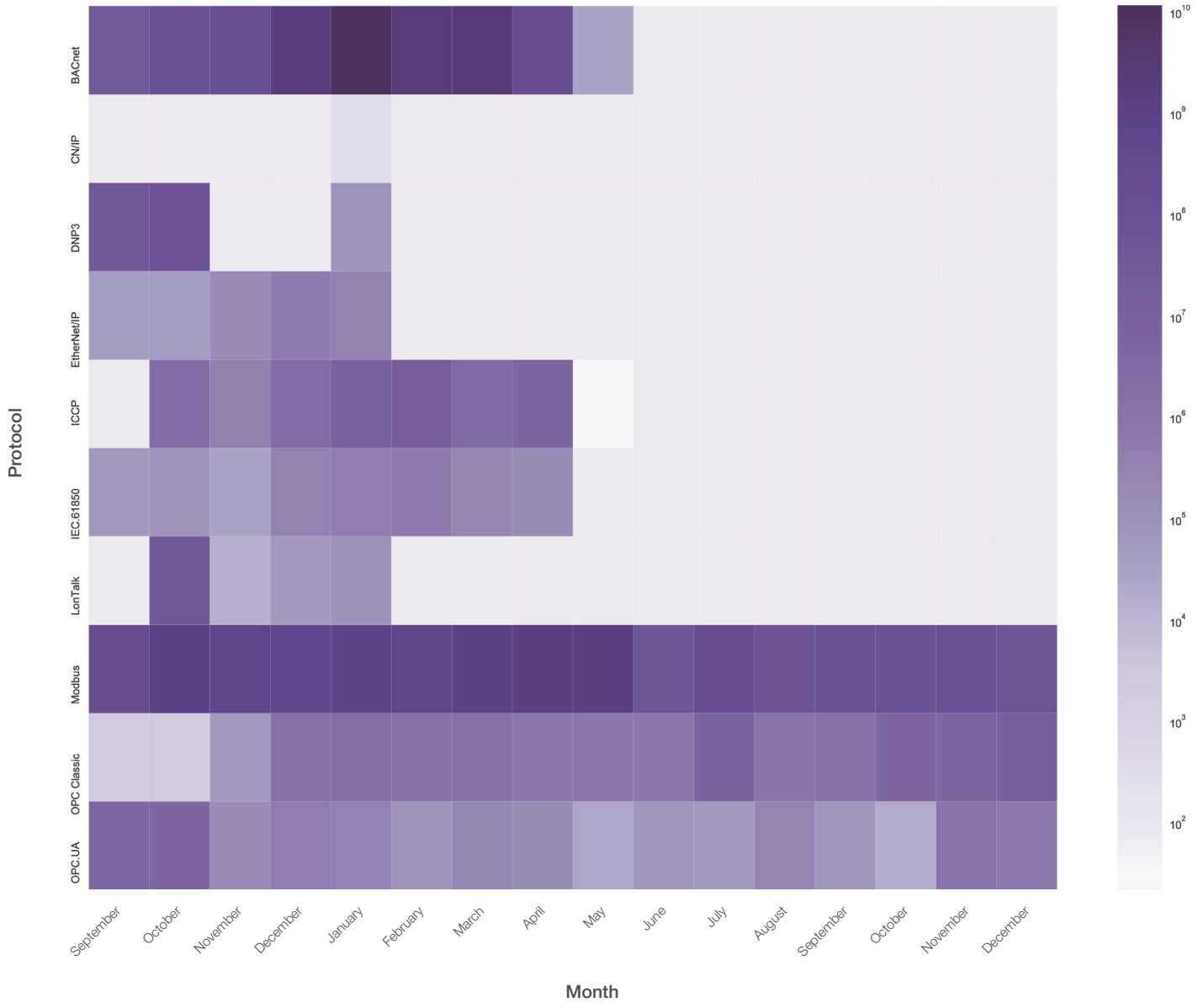


Figure 4: Volume of detections of protocol threats, September 2017 - December 2018.

.

The third most targeted protocol, **Modbus**, is a communications protocol that helps different components of OT systems interact effectively. This technology was developed in 1979 and was designed for a closed (i.e., air-gapped) system. Modbus has dozens of different iterations created by different vendors, making it difficult for OT teams to track its vulnerabilities.

No ICS/SCADA vendor is immune.

Attacks targeting each of the 70 OT vendors we track were detected in 2018, and apart from a handful of specific attacks (i.e., on Schneider and Moxa), these threats were found consistently throughout the year (Figure 5). That said, the most targeted vendors in terms of unique threats are some of the biggest: Advantech, Schneider, Moxa, and Siemens (Figure 6). As a general rule, older, more complex vendor offerings have more vulnerabilities than newer, more streamlined products.

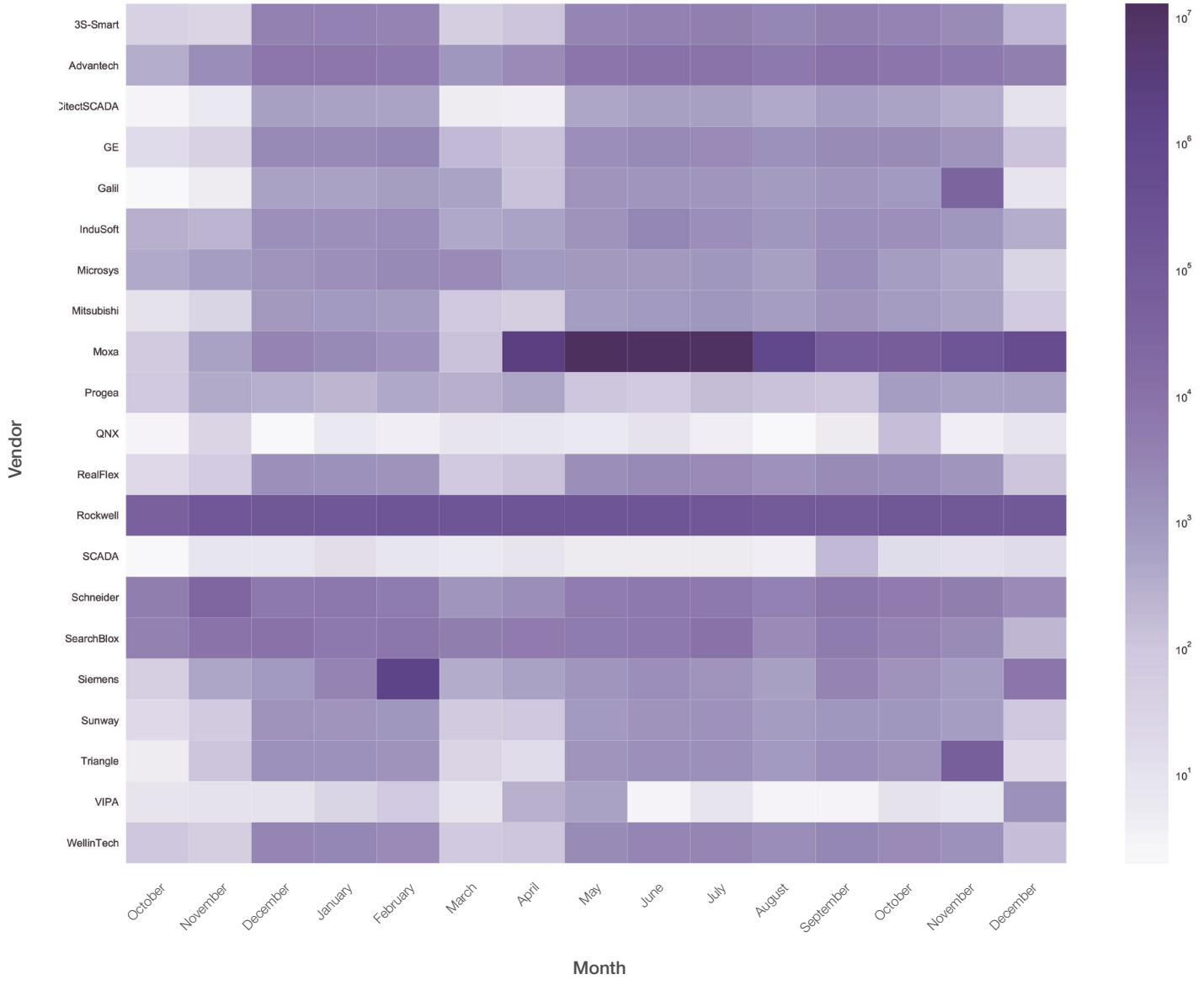


Figure 5: Volume of detections of threats targeting ICS/SCADA vendors, October 2017 - December 2018.

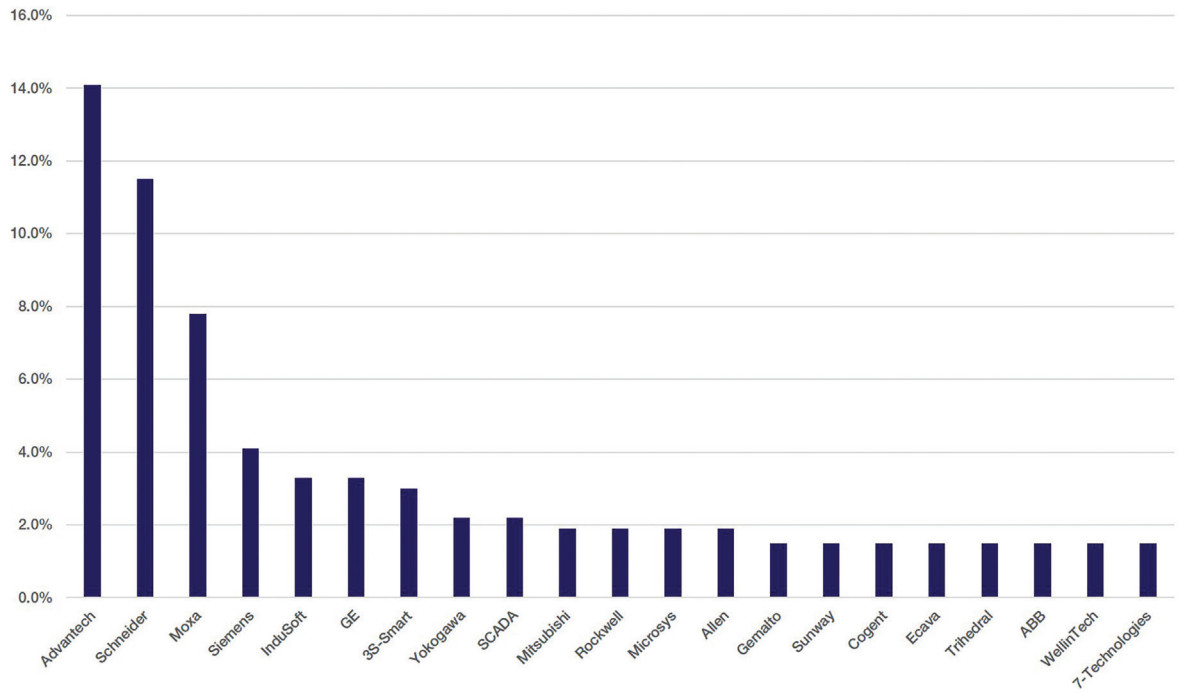


Figure 6: Top ICS/SCADA vendors, ranked by number of unique threats detected.

In all, IT-based attacks are increasing.

Despite seasonal fluctuations and a wide variety of targets, the data is clear on one thing: IT-based attacks on OT systems are increasing. For example, Figure 1 shows that the spike in new threats detected is much higher at the end of the year than the spike at the beginning of the year. And Figure 7 illustrates that exploits targeting almost every ICS vendor increased in both volume and prevalence over the course of 2018. There is no reason to expect this trend to change in 2019.

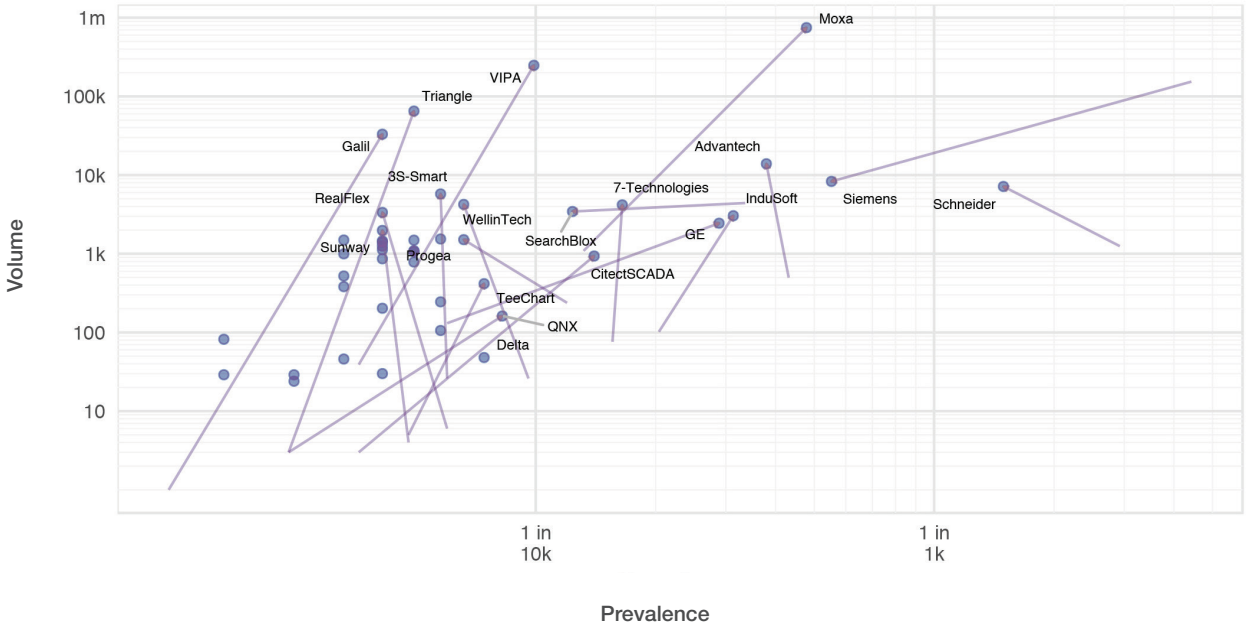


Figure 7: Change in prevalence and volume of exploits targeting the top ICS vendors, Q1-Q4 2018.

Trend: Attacks Specifically Designed for OT Systems Continue to Appear, and Safety Systems Are Now a Target

Malware targeted specifically at ICS and SCADA systems has been developed for a decade or longer, but examples are not numerous. OT-specific exploits include **Stuxnet, Havex, Industroyer,** and most recently, **Triton/Trisis.**

Industroyer and Havex are thought to have been initially used by Russian forces as cyber weapons targeting Ukraine's power grid during their takeover of the country in 2016. The malware has since leaked and been reutilized against various other grids where the same Schneider Electric infrastructure is found.[11]

A new and dangerous attack targets safety systems.

Triton/Trisis targets Triconex safety instrumented system (SIS) controllers, also sold by Schneider Electric and ubiquitous in the energy industry. Its first victim, an oil and gas facility in Saudi Arabia, suffered a full shutdown in 2017.[12] Given the fact that the malware targets the safety system, it could have been much worse—destroying machinery and threatening lives.[13] In April 2019, it was announced a second victim was hit by Triton/Trisis—an unnamed company in the Middle East.[14] Experts are alarmed by Triton/Trisis, which in many respects is the first true cyber-physical attack on OT systems.

Ransomware Continues to Attack OT Systems

In early 2018, FortiGuard Labs saw a dramatic increase in ransomware and ransom worms in IT environments.[6] This came on the heels of the massive and highly successful NotPetya ransomware attack in 2017, which brought both IT and OT systems to their knees around the world. Among OT systems affected:

- **Merck:** NotPetya shut down OT systems across most of the pharmaceutical giant, shutting down production and forcing the company to borrow $240 million worth of Gardasil doses from stockpiles maintained by the U.S. Centers for Disease Control (CDC).[7] All in all, the attack cost the company nearly $1 billion.
- **A.P. Møller – Maersk:** The world's largest container shipping company suffered a 20% drop in volume as a result of NotPetya—a figure that would have been much worse without valiant employees running the huge global operation manually and rebuilding an entire electronic infrastructure in 10 days.[8] The company is estimated to have lost at least $200 million from the attack.

As of late 2018, ransomware attacks on IT systems have declined and many threat actors appear to have "moved on" to other types of attacks like cryptojacking.[9] However, cyber criminals tend to recycle existing malware to attack OT systems—many of which are not as well protected as IT systems. This may suggest that ransomware will be a bigger threat for OT systems than for IT ones in the near term. Since SCADA masters often run on Microsoft Windows- and Linux-based hardware, ransomware threats can impact those machines if they are not adequately protected.

This scenario was confirmed by the March 2019 attack on aluminum giant **Norsk Hydro**, which shut down several plants and cost the company $40 million in the first week. While the **LockerGoga** malware involved in this attack is reportedly being refined and improved, its first manifestation was relatively basic and patterned after earlier malware.[10]

Attacks continue with older OT threats.

Data from FortiGuard Labs indicates that OT-specific malware continues to hit devices around the world. For example, Figure 8 indicates significant intrusion attempts using Industroyer in 2018, especially in the first half of the year. This data again suggests attempts to gain maximum value from existing malware, and continued danger that a cyber criminal will successfully take down a piece of critical infrastructure for an extended time.

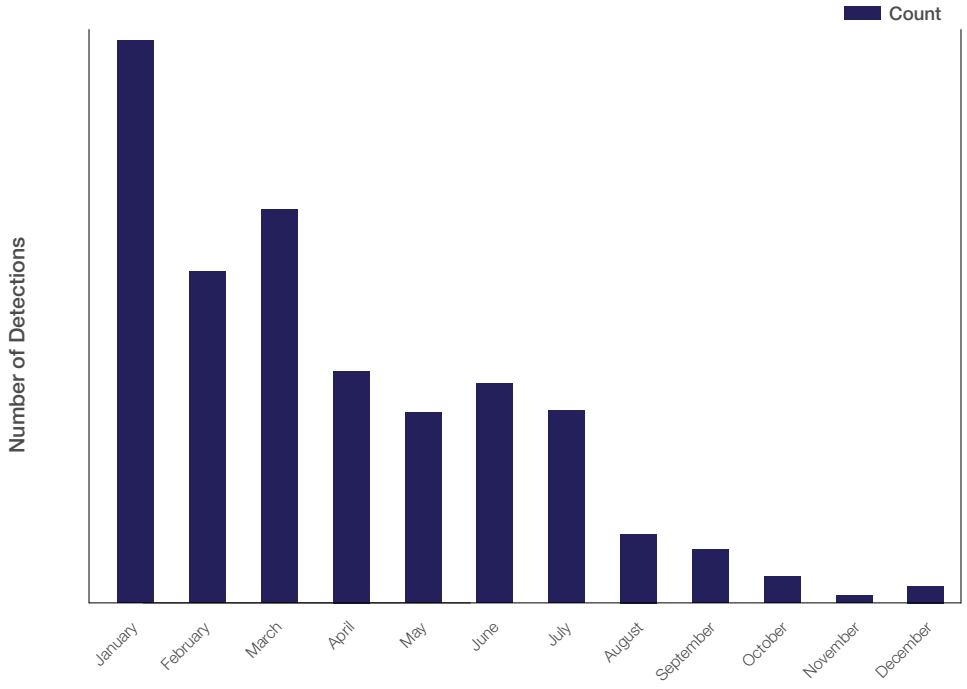


Figure 8: Detections of Industroyer malware, 2018.

EternalBlue: A Threat to Legacy Windows Systems

The U.S. National Security Agency (NSA) developed EternalBlue, according to testimony from former employees of the agency. On April 24, 2017, it was leaked by the Shadow Brokers hacker group and was used in the WannaCry and NotPetya ransomware attacks later that year. It is also thought to be a part of the Retefe banking Trojan. It exploits a vulnerability in Microsoft's Server Message Block (SMB) protocol.

Microsoft has upgraded SMB to a new protocol called Common Internet File Sharing (CIFS), so IT systems with updated Microsoft Windows infrastructure simply need to configure CIFS not to accept requests using the older SMB protocol. Unfortunately, many ICS/SCADA systems are based on older versions of Windows that do not support CIFS. This requires an external control to be placed in the next-generation firewall (NGFW) that allows certain types of SMB traffic but rejects other types.

Trend: OT System Attacks Transcend Geography

In a global economy dominated in many industries by global players and characterized by extreme connectivity, geography is easy to traverse for legitimate actors as well as criminals. Figure 9 indicates that while attacks targeting most vendors were relatively level from region to region, Rockwell and Schneider exploits disproportionately affected North America, while Siemens attacks were more frequent in Asia Pacific. In all three cases, this reflects where the strong markets are for each company. On the other hand, Moxa systems are ubiquitous and heavily targeted around the world, despite the Japan-centric nature of the biggest attack on its users—the Moxa 313 vulnerability (see "The Moxa 313 Vulnerability: An Intense Localized Exploit" on page 13).

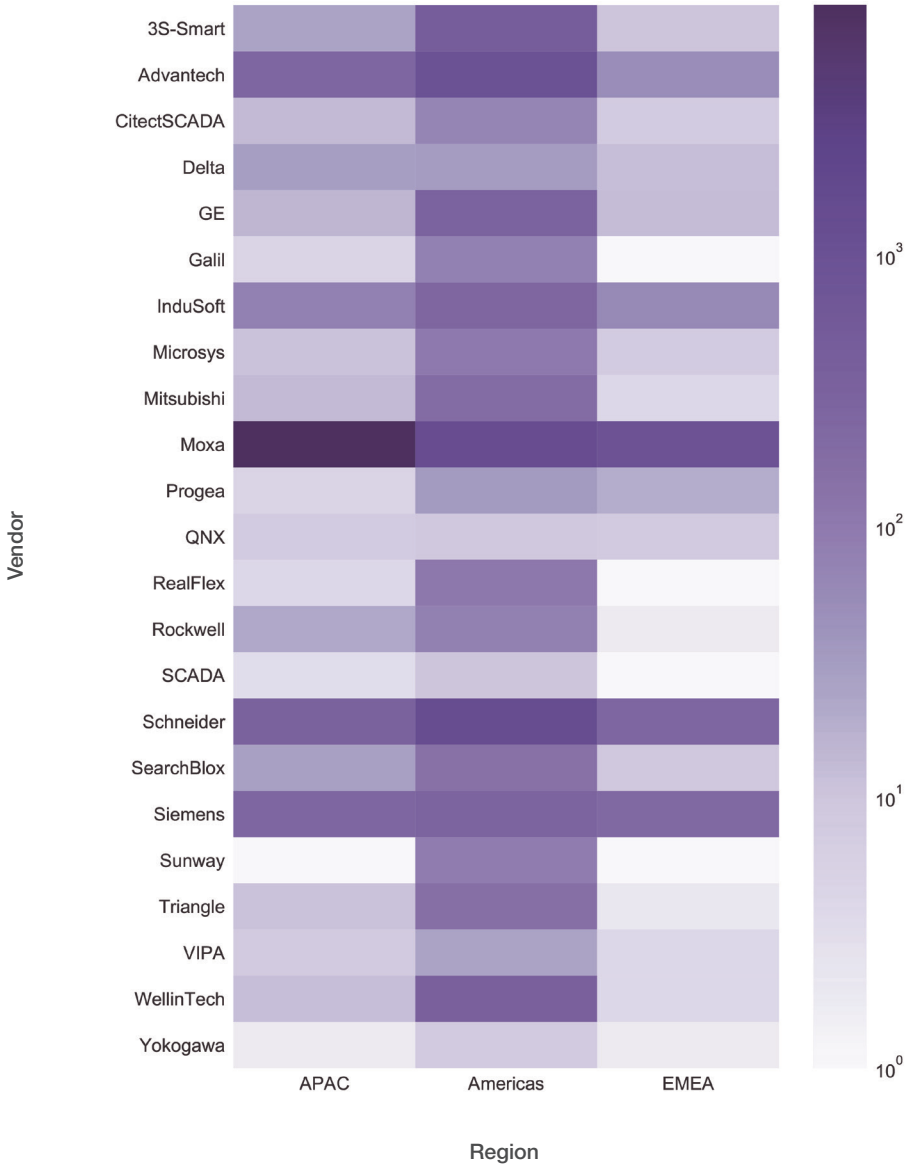


Figure 9: Regional distribution of detections of existing threats targeting specific ICS/SCADA vendors, 2018.

Figure 10 shows that while the BACnet and Modbus protocols were heavily targeted around the world, EMEA saw the most intense level of detections. The volume of attacks on machines using the other protocols was either fairly level across geographies or more focused in the areas where they are most commonly used. For example, ICCP is primarily used by vendors such as Siemens and Honeywell, which have a smaller footprint in Asia.

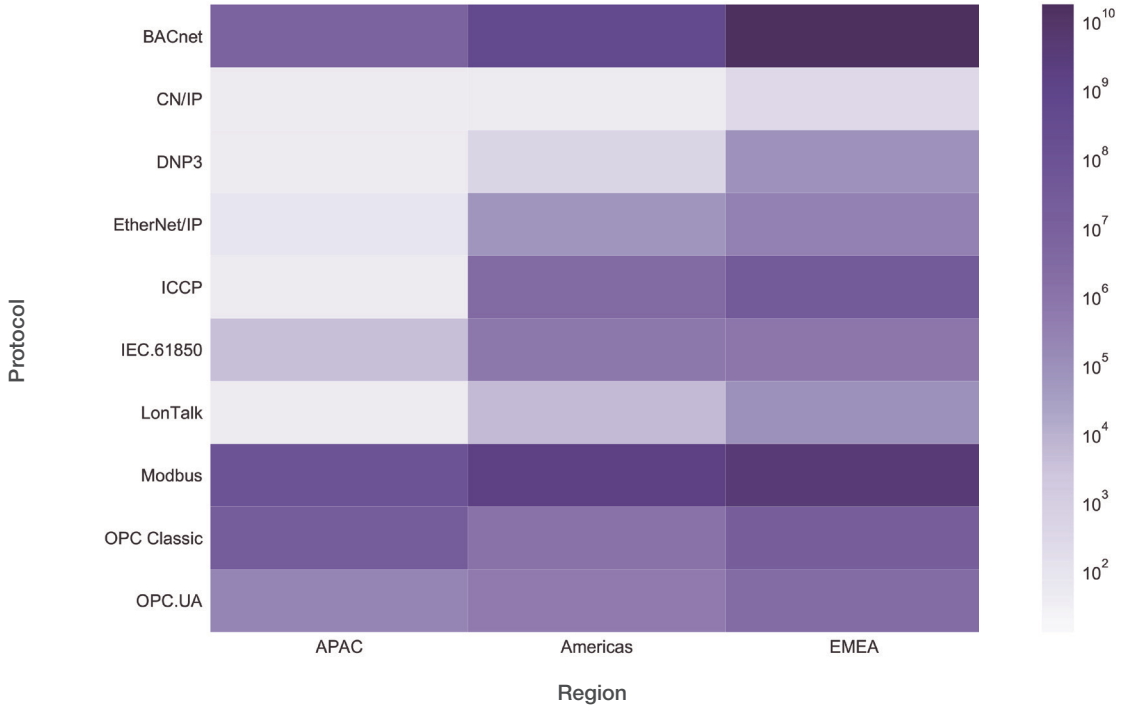


Figure 10: Regional distribution of overall detections of existing threats, 2018.

The Moxa 313 Vulnerability: An Intense, Localized Exploit

This attack, unveiled in April 2018, targeted an operating system command execution vulnerability in Moxa devices, in which the system failed to validate the input while processing a malicious Telnet request. It hit thousands of NGFWs in rapid succession during April, May, and June before disappearing almost entirely by September (Figure 11)—presumably due to the patching of systems against the threat.

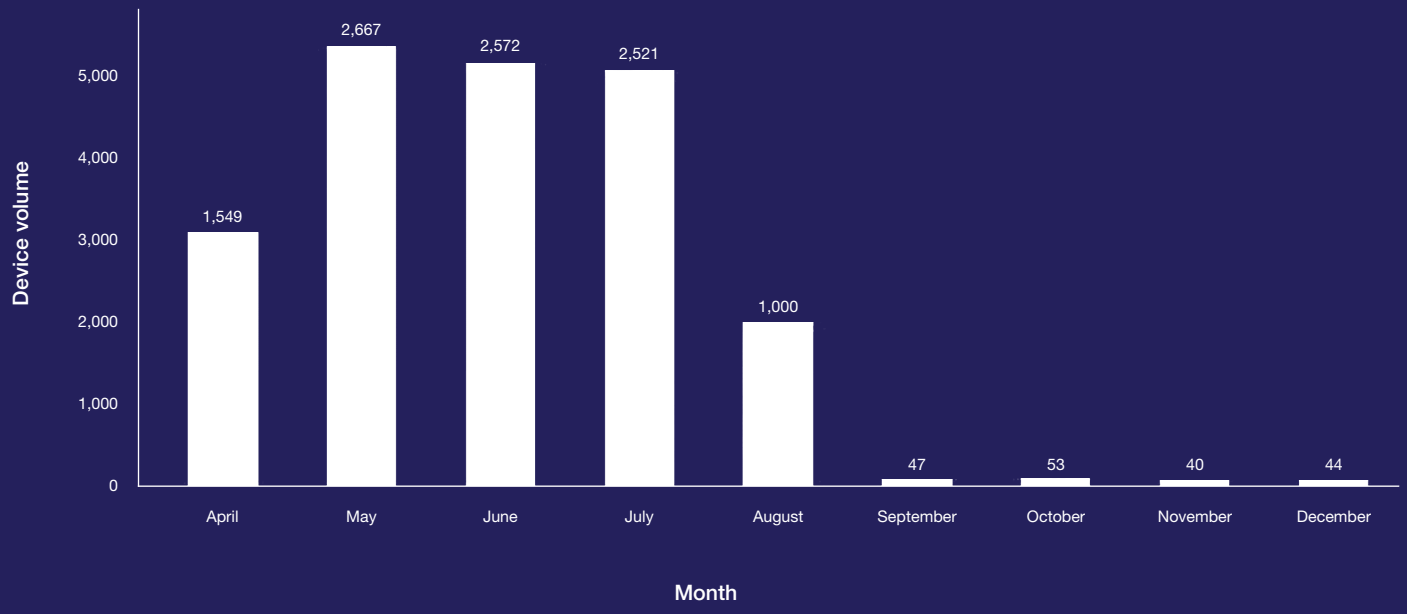


Figure 11: Moxa 313 detections by month, 2018.

Geographic analysis of this exploit reveals that the attack is almost completely confined to Japan (Figure 12), where Moxa technology is widely used in home and business automation products. However, Moxa is commonly used in other countries around the world. The fact that this attack spiked so quickly—even in an isolated geography—underscores the fact that threat actors tend to target the smallest and simplest portions of an OT infrastructure: the bridges and serial converters.

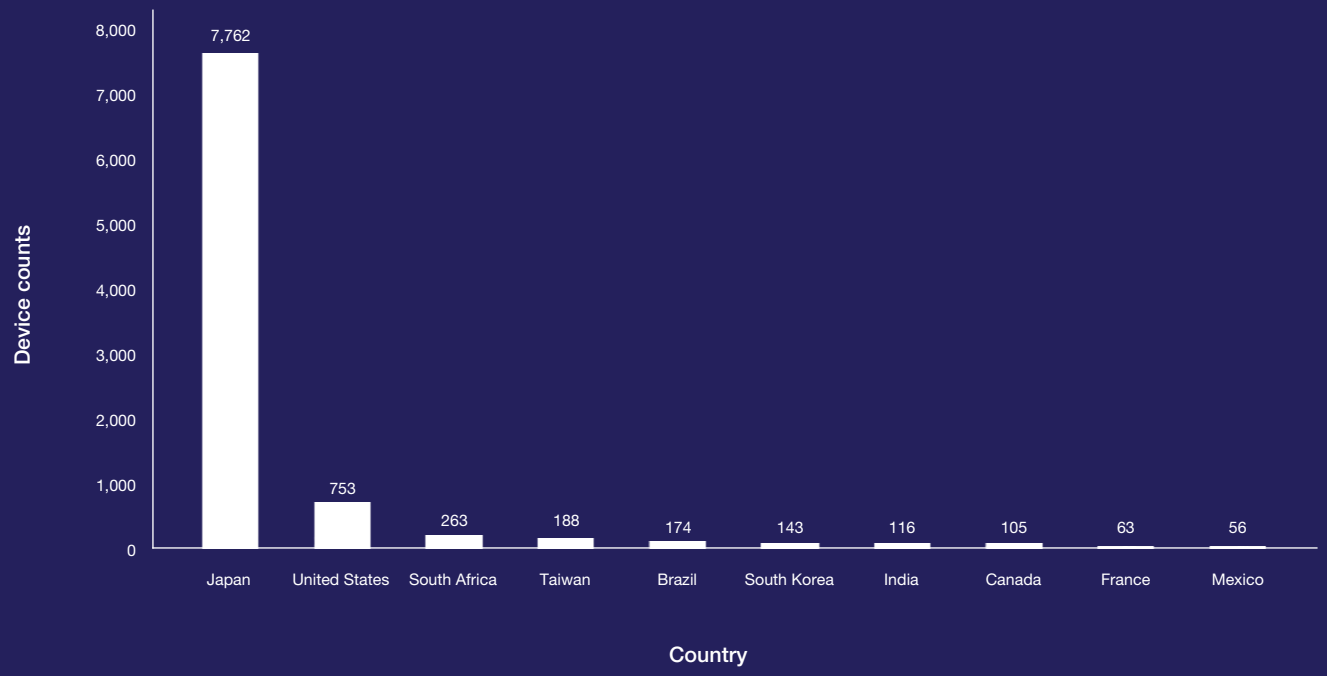


Figure 12: Moxa 313 detections by country, 2018.

Conclusion

The Fortinet 2019 Operational Technology Security Trends Report depicts a threat landscape that 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 in both older and newer technologies. The special challenges posed by slower replacement cycles and resulting legacy technology will not go away for a number of years.

The governments of the world are responding to these new threats, especially with regard to critical infrastructure. The risks are great, up to and including global economic collapse. In response, governments have developed guidelines to help industries protect their critical assets. For instance, the North American Electric Reliability Corporation (NERC) standards were instituted in response to the 2003 blackout in the northeastern United States. The fact that standards such as NERC and the National Institute of Standards and Technology (NIST) are becoming more stringent is one more indication that the threat is real.

ICS and SCADA systems have historically been the technology workhorses at many organizations, lasting for decades without major upgrades. The reality of advanced persistent threats requires a more strategic approach—everything from patching to segmentation to access control. It is imperative that those systems are subject to the same level of security protection, the same security hygiene standards, and the same tracking and reporting processes as the IT network. Otherwise, the OT network will be the weak link through which adversaries are able to infiltrate and gain access to critical systems and data—both OT and IT.

To make this happen, the IT and OT functions in every organization need to overcome the cultural challenges brought on by their past isolation. The groups must come to understand each other's values so that a mutually beneficial relationship can be forged for the future. The threats are real, and they will get bigger. The best way to counter them is with a comprehensive, strategic approach involving an entire organization.

References

[1] Barbara Filkins, "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," SANS Analyst Program, July 2018.

[2] Jeff Goldman, "IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices," eSecurity Planet, November 8, 2017.

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

[4] "Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks," Fortinet, May 7, 2018.

[5] Oliver Gasser, et al., "Security Implications of Publicly Reachable Building Automation Systems," Technical University of Munich, accessed April 18, 2019.

[6] "Quarterly Threat Landscape Report, Q4 2018," Fortinet, accessed April 9, 2019.

[7] Eric Palmer, "Merck has hardened its defenses against cyberattacks like the one last year that cost it nearly $1B," FiercePharma, June 28, 2018.

[8] Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz," The Register, January 25, 2018.

[9] "Quarterly Threat Landscape Report, Q4 2018," Fortinet, accessed April 9, 2019.

[10] Lindsey O'Donnell, "Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities," Threatpost, March 27, 2019.

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

[12] Lily Hay Newman, "Menacing Malware Shows the Dangers of Industrial System Sabotage," WIRED, January 18, 2018.

[13] "FortiGuard Threat Intelligence Brief," Fortinet, February 2, 2018.

[14] Tara Seals, "SAS 2019: Triton ICS Malware Hits A Second Victim," Threatpost, April 10, 2019.

FORTINET

www.fortinet.com

May 8, 2019 9:31 PM

D:\Fortinet\Packaged files\2019\May\report-security trends Folder\report-security trends

352048-0-0-EN