

2020 Report on Threats Affecting ICS Endpoints

Matsukawa Bakuei, Ryan Flores, Lord Remorin, Fyodor Yarochkin



TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

**Matsukawa Bakuei,
Ryan Flores, Lord Remorin,
Fyodor Yarochkin**

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963-2017)

Contents

4

Executive Summary: Findings

5

Definitions and Disclosure

8

Malware Threats Affecting
Endpoints Running ICS Software

17

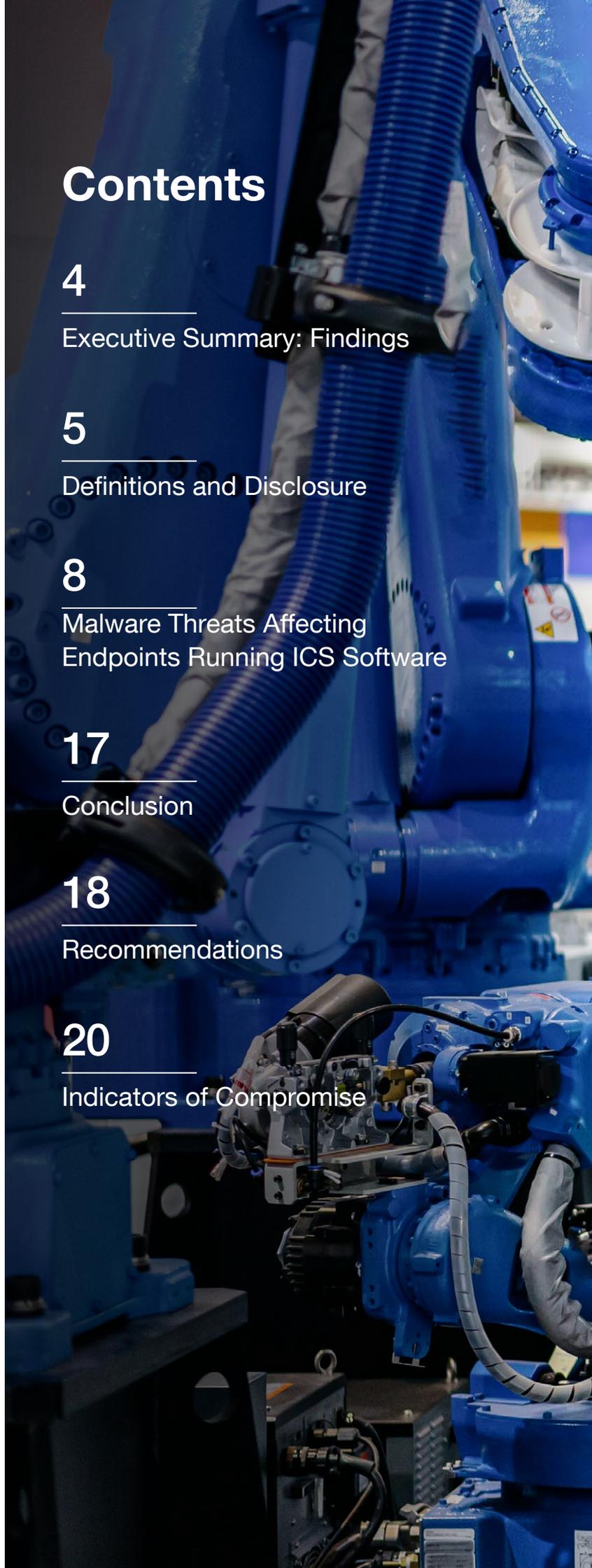
Conclusion

18

Recommendations

20

Indicators of Compromise





The security of Industrial Control Systems (ICS) has been pushed into the limelight over the past few years due to the increasing interconnection between the business process on the IT side and the physical process on the OT side. While this interconnection improves visibility, efficiency, and speed it also inadvertently exposes ICSs to threats that have been affecting IT networks for decades.

To validate ICS security and establish a global baseline for examining the threats that plague these systems, we analyzed and reported specific malware families found in ICS endpoints.

The type of malware cybercriminals choose to wield in particular incidents offers a glimpse into the scope and severity of these cyberattacks, providing clues on two key aspects: the attackers and the affected network.

The choice of malware helps unveil the attackers' motivation and skill level. For example, the use of ransomware or a coinminer signifies financial motivation, the use of a wiper or other destructive malware suggests sabotage, and the use of a backdoor or information-stealing malware reveals espionage. In terms of the attackers' skill, the use of customized malware suggests high technical skill or understanding of the attacked environment, while off-the-shelf malware suggests amateur skills, although this is not always the case.

The malware found in the system could also provide insights into the affected network's environment and cybersecurity hygiene. We can infer the inadequate security practices applied on the affected networks based on malware infections found in them. For one, malware variants exploiting certain vulnerabilities imply unpatched endpoints. On the other hand, file-infecting viruses suggest previous infections that were not totally eradicated, with groups of unchecked devices hosting the viruses.

By identifying and breaking down the malware threats found in ICSs through the data we gathered in 2020, we hope to provide insights into the general security posture of industrial control systems found in IT/OT environments and what attackers are doing once they compromise it. We also share recommendations on how to secure these environments.

Executive Summary: Findings

1. Ransomware remains a concerning and rapidly evolving threat to ICS endpoints globally. Major ransomware families affect ICS endpoints, and the US is one of the most targeted countries for these attacks.
2. Coinminers affect ICSs mostly through unpatched operating systems. Since ICS endpoints are still vulnerable to the EternalBlue vulnerability, coinminers that were distributed through Equation Group tools¹ exploiting this vulnerability is rampant in several countries, especially in India.
3. Conficker is still propagating on ICS endpoints running newer operating systems. Variants of Conficker with the additional routine of brute-forcing admin shares can infect ICS endpoints even if they are running an OS that is not vulnerable to MS08-067, a Windows Server Service vulnerability that Conficker can use as an attack vector.
4. Legacy malware continues to thrive in IT/OT networks. Despite being relatively older types of malware, worms, such as Autorun, Gamarue, and Palevo, which propagate through removable drives, are still commonly detected in ICS endpoints.
5. Malware detected on ICS endpoints varies between countries. By percentage, Japan had the least amount of ICS endpoints affected by malware or potentially risky software, while China has the most such detections (of the top 10 countries). As mentioned earlier, the US had the most ransomware infections, while India had the most coinminer infections.

Definitions and Disclosure

IT/OT Network

This pertains to the convergence of the IT and the OT network; the connection of the business process on the IT side with the physical process on the OT side. This link enables data exchange, as well as the monitoring and control of the operations from the IT network. For this research, the data comes from ICS endpoints that are part of the IT/OT network and does not include ICS endpoints from air-gapped systems or those without an internet connection.

ICS Endpoint

IT/OT networks use ICS endpoints in the design, monitoring, and control of industrial processes. These ICS endpoints have specific software installed on them that performs important ICS functions. Examples of these software are:

- Industrial automation suites, such as Siemens' Totally Integrated Automation, Kepware's KEPServerEX, and Rockwell Automation's FactoryTalk.
- Engineering Workstation (EWS), which is used in the programming of an industrial process or workflow. This includes:
 - Control systems such as Mitsubishi Electric's MELSEC GX Works or Phoenix Contact's Nanonavigator
 - HMI (Human Machine Interface) such as MELSEC GT Works or Schneider's GP-PRO EX
 - Robot programming software such as ABB Robotstudio
 - Design software such as Solidworks
 - Historian software such as Honeywell's Uniformance
 - Supervisory Control and Data Acquisition (SCADA) such as Siemens' Simatic WinCC SCADA
 - Field device management and configuration such as PACTware and Honeywell's EZconfig
 - Converters for serial to USB connections such as Moxa's Uport

These ICS endpoints can be found in various levels of the IT/OT network architecture, except the process and control level. All the identified ICS endpoints were running Windows operating systems.

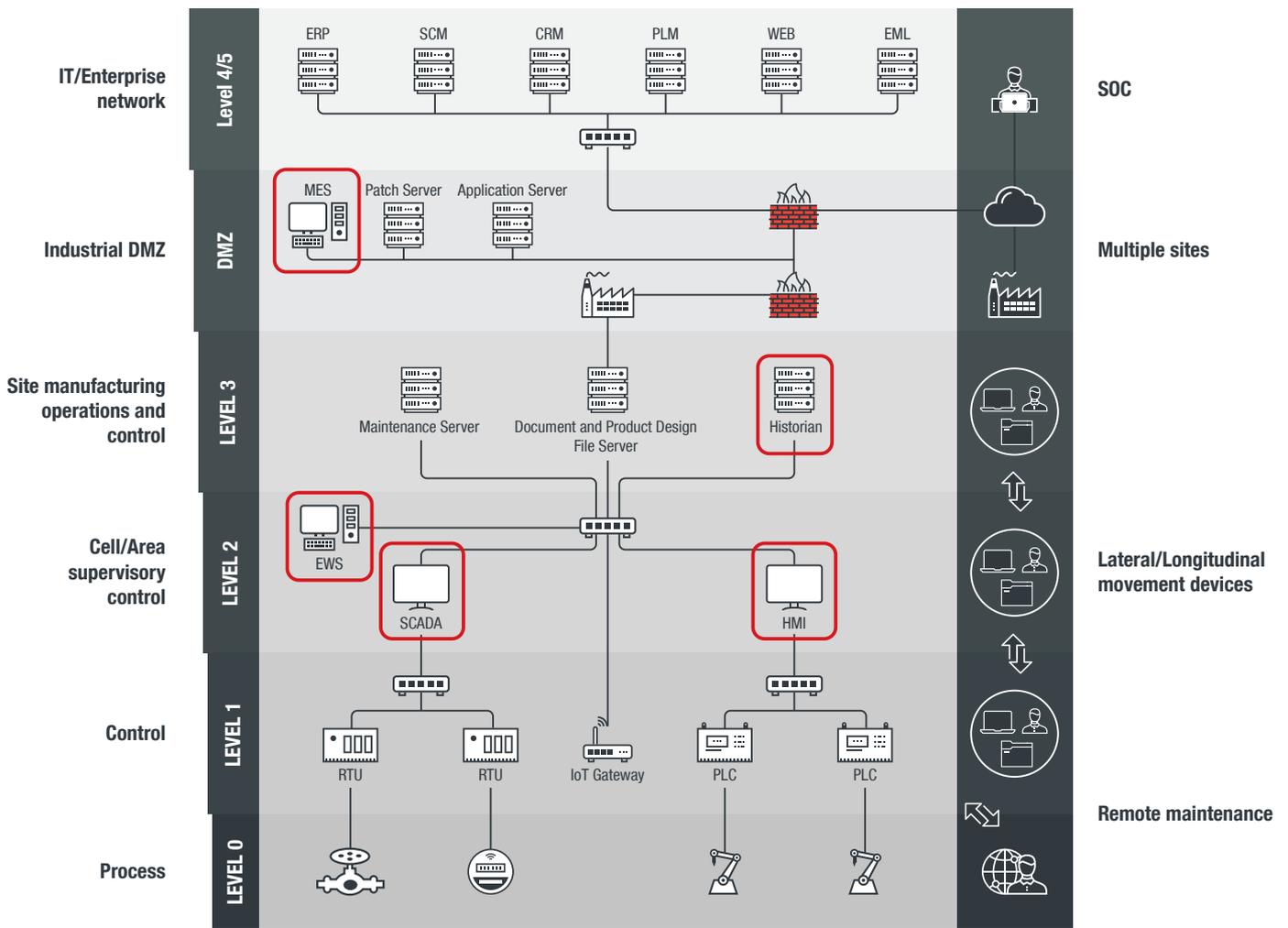


Figure 1. ICS endpoints, highlighted, as shown in a Purdue model architecture

While we know that these endpoints are running ICS software, there is no guarantee that they are controlling industrial processes. Some of these endpoints might have been set up for training or testing purposes. However, we made sure to filter out obvious test machines, endpoints used by penetration testers, and endpoints coming from universities, so we can confidently say that the majority of our data comes from real ICSs and that the malware detection data is not skewed by penetration testers, researchers, and student machines.

Disclosure

We identified ICS endpoints using a mix of indicators such as file names, file paths, and processes that were reported to the Trend Micro™ Smart Protection Network™. Processing of relevant data points was done in compliance with Trend Micro's Data Collection Disclosure policy, and the customer's anonymity is maintained throughout the whole process.

Users can opt out of data collection by disabling the Certified Safe Software Service, Smart Scan, and Behavior Monitoring features from the product administration console. However, this will disable the benefit of having up-to-the-second threat protection afforded by the Smart Protection Network.

Please note that these detection numbers are from the coverage of the SPN sensors distributed globally, which is not exhaustive. Those regional rankings and figures cannot be free from such market-share-influenced distribution bias.

Malware Threats Affecting Endpoints Running ICS Software

Post-Intrusion Ransomware

We saw a significant rise in ransomware activity affecting industrial control systems in 2020, mostly due to increased Nefilim, Ryuk, LockBit, and Sodinokibi attacks from September to December. Together, this group of ransomware makes up more than half of ransomware attacks affecting ICSs in 2020.

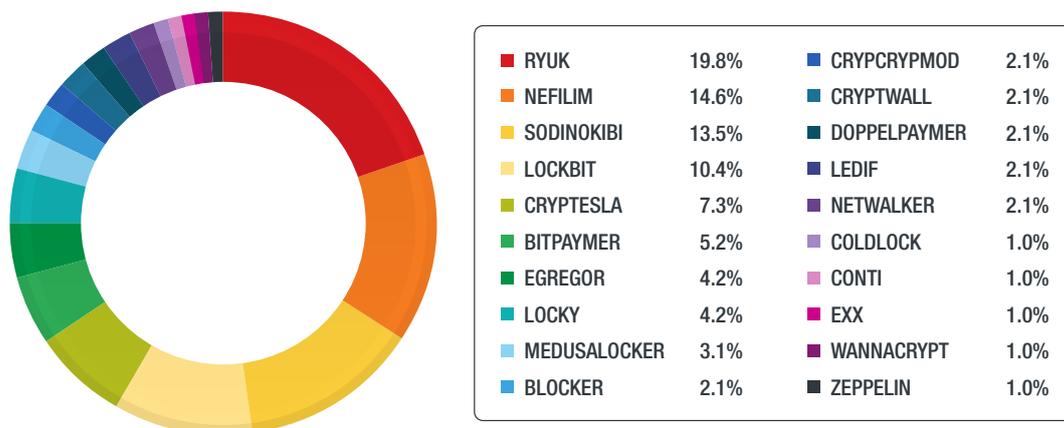


Figure 2. Breakdown of ransomware that affected industrial control systems in 2020

Source: Trend Micro™ Smart Protection Network™ infrastructure

The US is by far the country with the most ransomware detections affecting ICSs, with India, Taiwan, and Spain a far second.

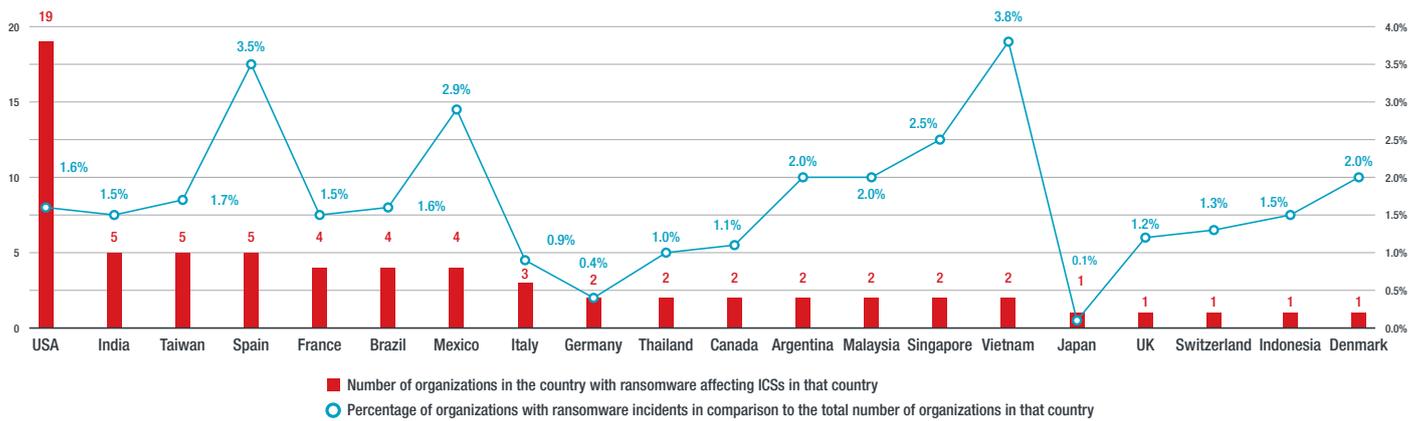


Figure 3. Per country breakdown of organization-related ransomware detections for industrial control systems in 2020

Source: Trend Micro™ Smart Protection Network™ infrastructure

The US is a big country, with a vast number of organizations that can fall victim to ransomware. If we take the percentage of organizations running industrial control systems that had ransomware affecting their systems, Vietnam, Spain, and Mexico actually makes up the top three.

Interestingly, Vietnam’s ransomware detections were residual infections of GandCrab, a ransomware that was seen targeting Vietnam in 2018,² but has since been mainly out of sight — likely because of its distributor’s arrest in 2020.³

Ransomware in ICSs can cause the loss of view or control of physical processes. Monitoring and control interfaces such as HMIs and EWS are reliant on image files (.jpg, .bmp, .png) and configuration files to render the interface; However, in ransomware attacks, data including configuration files and images end up encrypted, and therefore, unusable by the ICS software. Therefore, ransomware effectively cripples⁴ the HMI and EWS.

This in turn leads to productivity and revenue losses for the facility. In fact, when we operated a fake factory as a honeypot,⁵ we experienced several days of downtime while recovering from ransomware incidents. This is the impact caused by ransomware affecting the ICS responsible for monitoring and control of industrial processes.

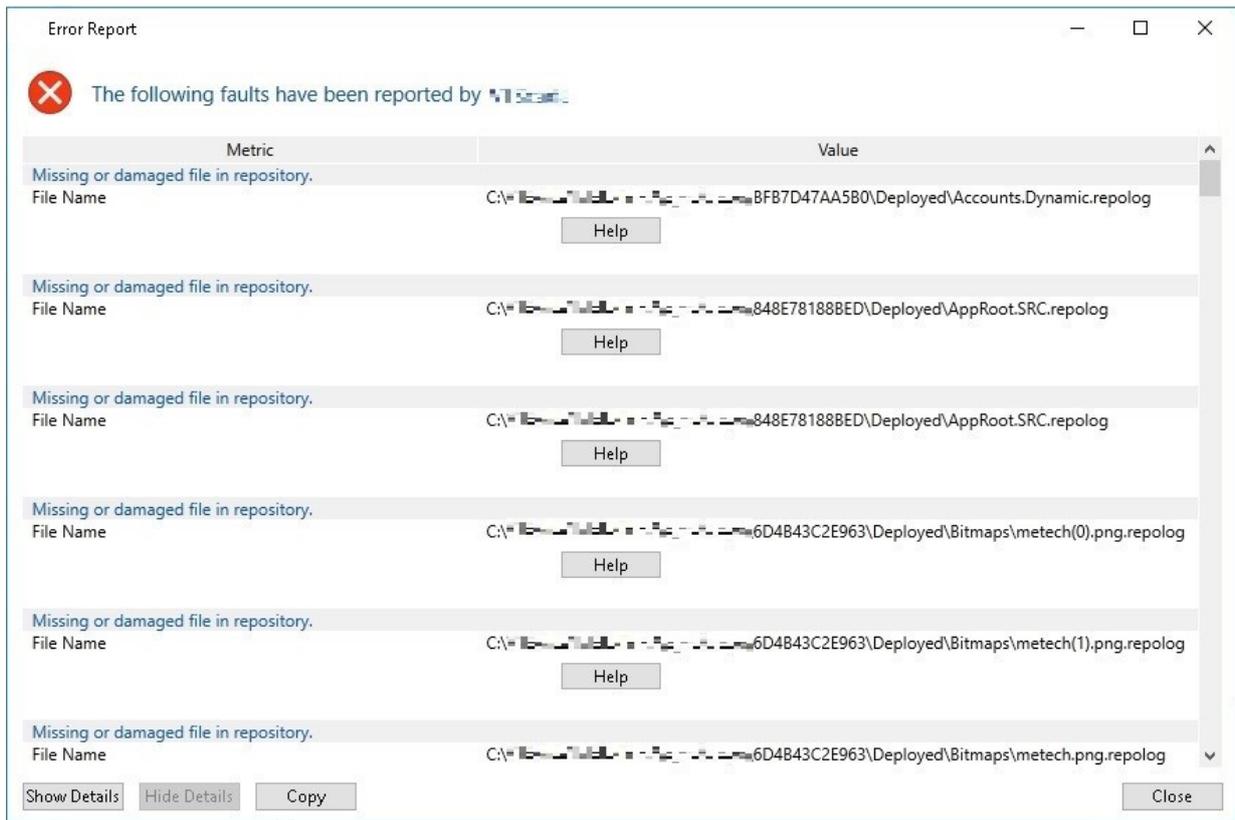


Figure 4. An HMI failing to load because the configuration files and image files used by the HMI were rendered unreadable by the ransomware

Image Credit: Trend Micro⁶

Another aspect of ransomware attacks that affect ICSs is the recent trend of double extortion,⁷ wherein the target files are not only encrypted but also exfiltrated and publicized. This especially affects ICS components dedicated to the design and development of industrial processes. Designs, programs, and documents such as supplier lists, parts lists, and industrial recipes contained on EWS, if successfully exfiltrated and received by the wrong party, can provide attackers with confidential information or proprietary product designs. For example, threat actors behind the Sodinokibi ransomware that affected Quanta, a major Apple supplier, threatened to release some of the documents that they managed to steal. The documents reportedly include new schematics for the upcoming iMac and Macbook Air.⁸

Coinminer

Aside from ransomware, coinminers are another financially motivated malware affecting ICSs. While a coinminer's code is not designed to destroy files or data, the mining activity's CPU utilization can adversely affect ICS endpoint performance. In our factory honeypot research,⁹ we have experienced unresponsive ICS endpoints after attackers installed coinminers in them. Indirectly, a coinminer can cause loss of control and view over an ICS, especially if those computers have low CPU capacity and/or running outdated operating system, a setup that is not rare in industrial environments.

The top coinminer family found on industrial control systems for 2020 is MALXMR, a post-intrusion coinminer. It was usually installed through fileless techniques, but starting in 2019, we have seen MALXMR infections that use Equation group tools to exploit the EternalBlue vulnerability to aid distribution and lateral movement.

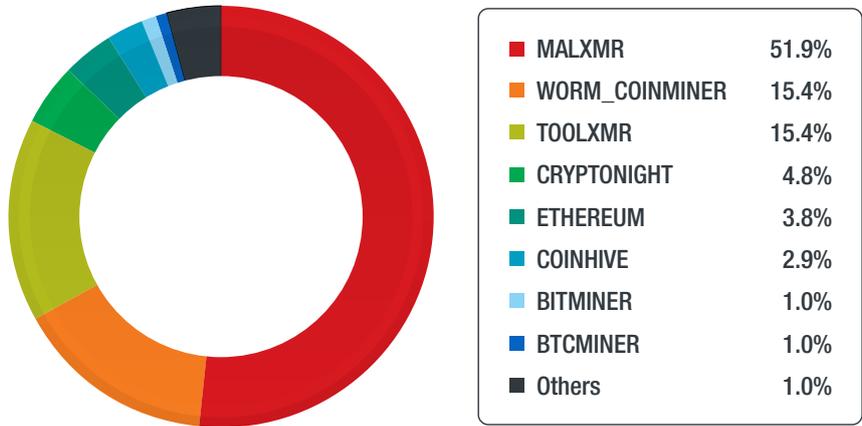


Figure 5. Breakdown of coinminers affecting industrial control systems in 2020

Source: Trend Micro™ Smart Protection Network™ infrastructure

Of the countries with MALXMR running on ICS endpoints, India accounts for more than a third of detections. However, this does not mean that India is specifically being targeted by MALXMR gangs to run their cryptominers. A look at WannaCry ransomware infections showed that India also had more than a third of WannaCry infections on ICS endpoints.

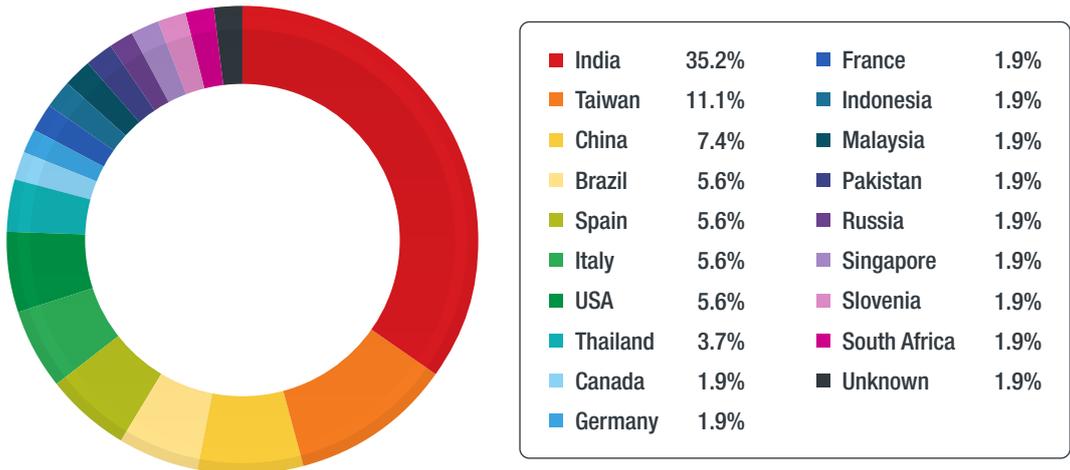


Figure 6. MALXMR distribution per country and organization

Source: Trend Micro™ Smart Protection Network™ infrastructure

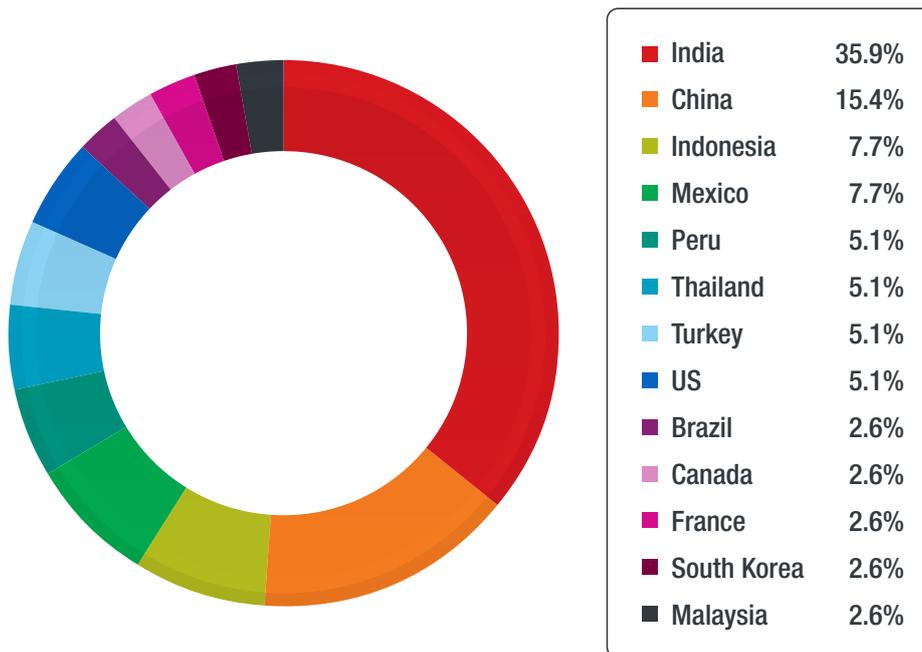


Figure 7. WannaCry distribution per country and organization

Source: Trend Micro™ Smart Protection Network™ infrastructure

This suggests that India has the most MALXMR infections because a lot of computers running ICS software are vulnerable to EternalBlue, as Equation group tools used by MALXMR and WannaCry both exploit the said vulnerability. This data shows how a country's general patch level makes it susceptible to certain threats.

Conficker

Similar to what we found from previous research on manufacturing environments,¹⁰ we still see Conficker (aka Downad) as a persistent threat for ICS endpoints. First discovered back in 2008, this computer worm is still being persistently detected on 200 unique endpoints.

We found that at least 94% of the endpoints we analyzed were running Windows 10 and Windows 7 operating systems. The most widely known propagation method of Conficker is exploiting the MS08-067 vulnerability that could allow remote code execution if an affected system received a specially crafted Remote Procedure Call (RPC) request.¹¹ But MS08-067 does not apply to Windows 10 and Windows 7, which leads us to the conclusion that these infections are propagated using either removable drives or dictionary attacks on ADMIN\$ share.

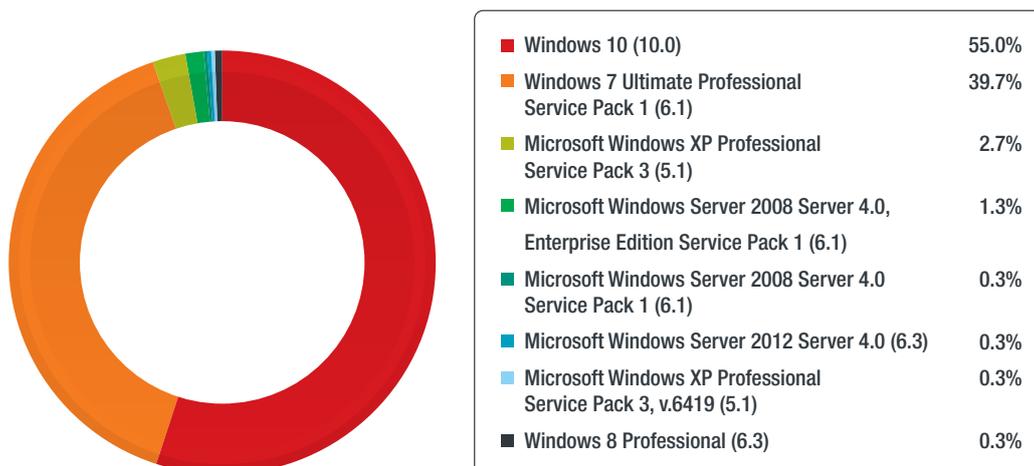


Figure 8. OS distribution of ICS endpoints with Conficker detections

Source: Trend Micro™ Smart Protection Network™ infrastructure

In relation to the preceding assumption, we found that at least 85% of the Conficker detections were detected from removable drives and at least 12% of the detections were found only on the Windows system directory. This indicates a successful Conficker infection even though the infected machine is not vulnerable to MS08-067. Trend Micro detects the majority of infections from the Windows system directory as WORM_DOWNAD.EZ and WORM_DOWNAD.AD (details on these detections can be seen in the Appendix Section of this paper). These are unique Conficker variants that have the additional capability to drop a copy of itself into ADMIN\$\system32 using the credentials of a logged-on user or by launching a dictionary attack¹² using common passwords. This is an interesting finding as it means that even though the endpoint is running a more recent version of Windows that is not susceptible to MS08-067, they still experienced a Downad infection because of weak admin credentials.

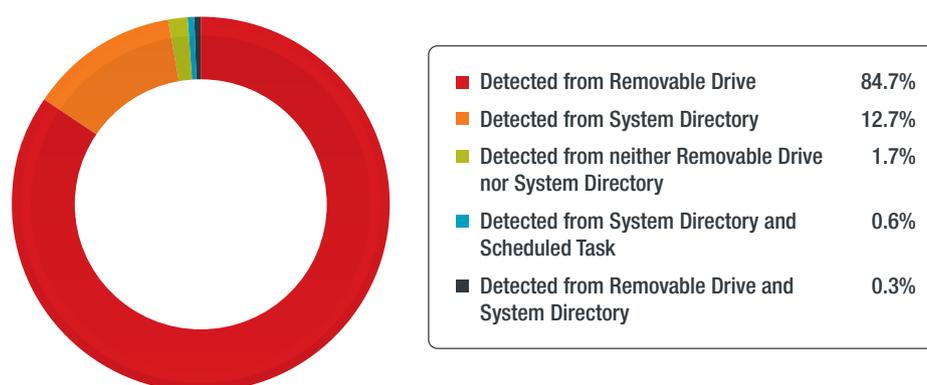


Figure 9. Location of Conficker detections based on file path

Source: Trend Micro™ Smart Protection Network™ infrastructure

Containing worm outbreaks is a difficult task and this scenario shows how multiple methods of propagation (network exploit, removable drives, and credential brute-force) make eradication difficult. Security personnel must make sure all methods of propagation are properly addressed. In this case, patching (or virtual patching), scanning removable drives for malware, securing network shares, and having an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) that can detect and prevent brute-force login attempts, are needed.

Legacy Malware

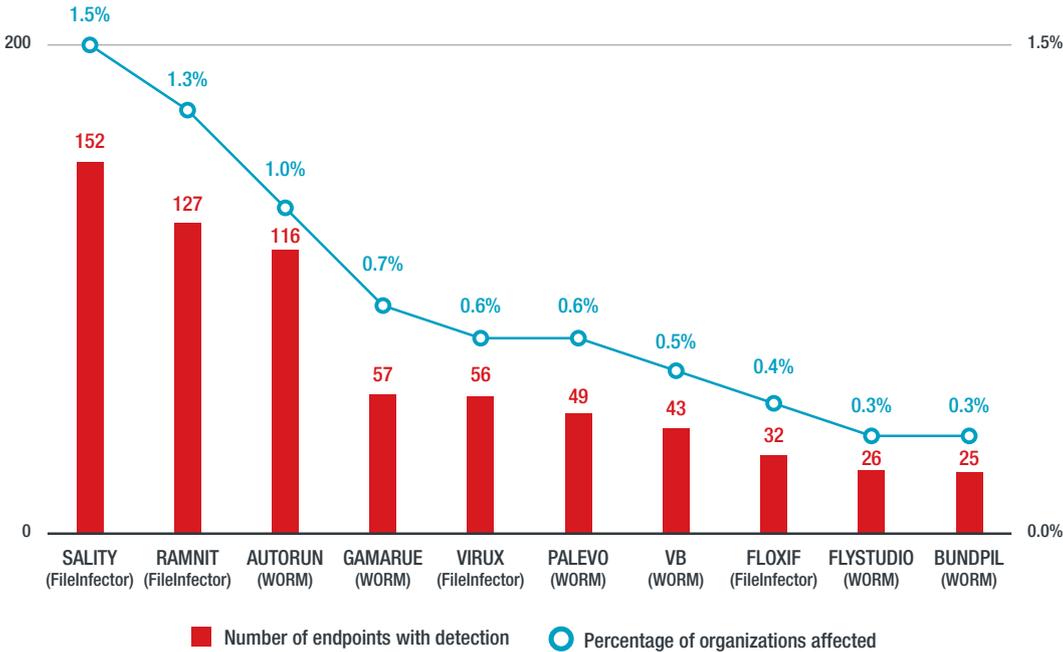


Figure 10. Breakdown of legacy malware detected in ICS endpoints

Source: Trend Micro™ Smart Protection Network™ infrastructure

In networks running ICSs, we detected old worm malware whose primary method of propagation is via network shares or removable USB drives. Even though these legacy malware are found in less than 2% of organizations, they are detected frequently and on several endpoints within the same network, signifying a localized outbreak.

Worms like Autorun, Gamarue, and Palevo became rampant in 2013 and 2014 but have since waned as security policies that disable autorun (that is, executable files declared in autorun.inf is automatically executed when a removable device is connected) have become widely adopted. While it is unsurprising to see these old, legacy worms in IT/OT environments, there are a couple of practices that contribute to the situation. First, transferring files and data via USB thumb drives is usually performed as a convenient solution for bridging air-gapped networks; however, this allows the propagation of such legacy worms. Second, asset owners create system backups or cold standby terminals and store them in removable drives but do not perform security scans against the package that might harbor malicious software.

The same goes for file infecting viruses found in ICSs. The similar conditions that made worms survive in air-gapped networks also allowed the likes of Sality, Ramnit, and Virut to thrive in those environments. These file infecting viruses are even older than removable drive worms, with some Virut variants dating back to 2009.

While these legacy worms and viruses are not associated with any cybercrime group or state-sponsored attackers, their continued presence in IT/OT networks suggests inadequate security and poor maintenance of data backups and removable drives. This has not only made the eradication of these viruses much more difficult, they also provide a secluded haven for legacy malware to survive, as evidenced by several endpoints detecting multiple legacy malware in the same removable drive.

This also proves how removable drives can be a major weak point on these ICS endpoints, something that a more advanced piece of malware, Stuxnet, took advantage of in attacks that targeted Supervisory control and data acquisition (SCADA) systems.¹³

Malware and Grayware Detections in the Top 10 Countries

This section focuses on malware and grayware (like potentially unwanted applications, adware, and hacking tools) detections in the top 10 countries with the greatest number of IT/OT networks with ICS endpoints.

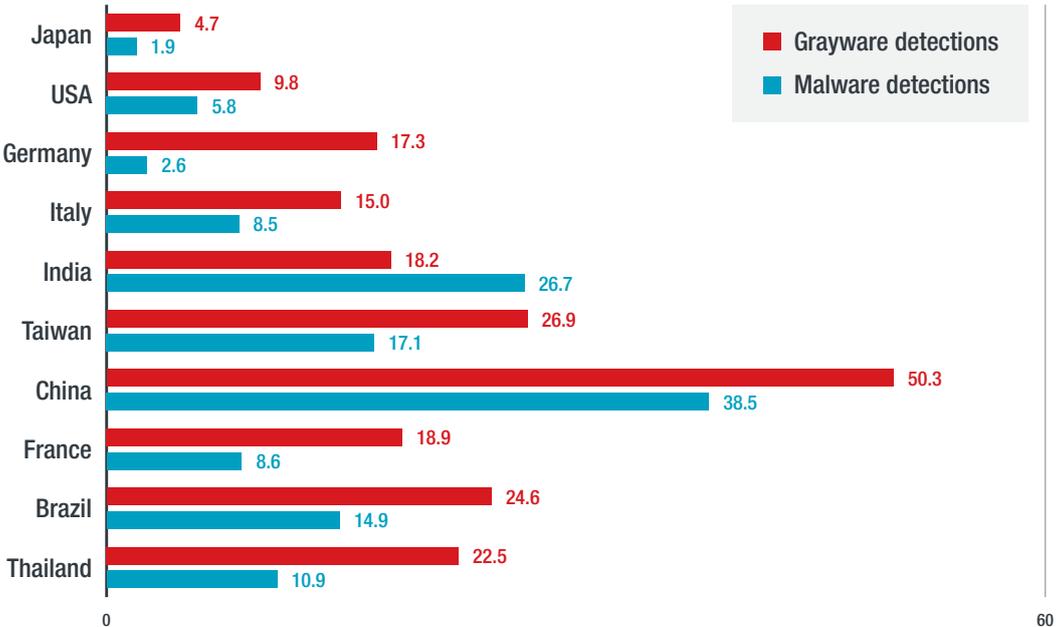


Figure 11. Top 10 countries' percentage of industrial control systems with malware and grayware detections

Source: Trend Micro™ Smart Protection Network™ infrastructure

The chart above shows the percentage of ICS endpoints that have malware or grayware detections for 2020. Japan had the least amount of IT/OT networks with malware and grayware detections, while China has the most malware and grayware detections.

Examining from a geographical point of view, we can see that some threat types affect certain countries more than others. As already highlighted in the earlier sections, the US had the most number of organizations affected by ransomware (Figure 12, in lilac).

Legacy malware (particularly worms in removable drives and file infecting viruses) had the most detections in India, China, the US, and Taiwan. India has the most coinminer, Equated malware, and WannaCry ransomware detections.

Japan has the greatest number of Emotet infections. But while Emotet is known to deploy Ryuk, Trickbot, or Qakbot post-infection, the said data seems to show no further installation of malware. ICSs in Germany have the most adware, mostly because of adware bundled with software tools.

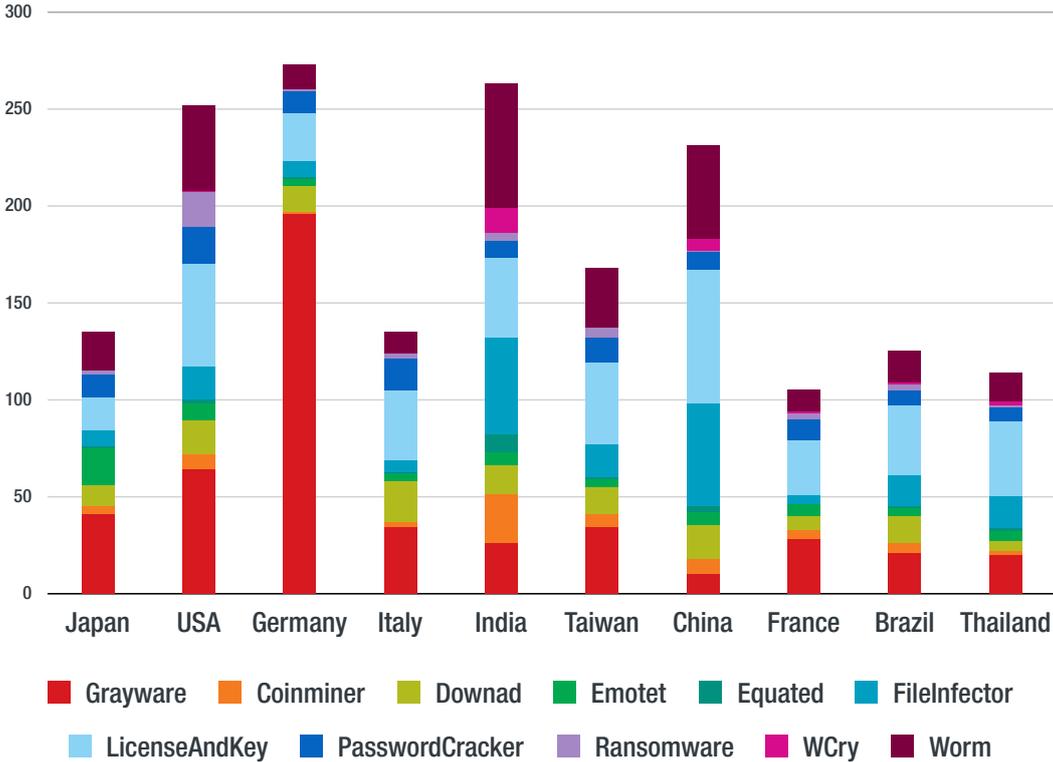


Figure 12. Top 10 countries breakdown of detections according to type

Source: Trend Micro™ Smart Protection Network™ infrastructure

Conclusion

Using malware detections as one of the criteria of IT/OT networks' cybersecurity readiness can improve their security posture and, in turn, better protect ICS endpoints. This prevents unintended downtime and the loss of view and control.

Based on the detection data, we can conclude that modern malware such as ransomware and coinminers and legacy malware such as file infecting viruses and worms both affect industrial control systems. This implies that both modern techniques (such as fileless malware, living-off-the-land, and hacking tools), as well as those by tried-and-tested legacy methods (old network exploits, removable drive autorun, network share bruteforcing, and file infection), can successfully infect ICS endpoints.

However, the stakes are higher in some attacks. For ransomware, organizations should be wary of cybercriminals' big-game hunting,¹⁴ where attackers first identify whom they were able to compromise, and then identify the key systems in the network to cause the most disruption and coerce the victims into paying. The presence of ransomware in ICSs in several attacks might indicate the attackers are starting to recognize these systems and are actively targeting them.

This means security should be a major consideration when interconnecting the IT network with the OT network.¹⁵ Security issues that are used by both the legacy malware and the latest attack trends should be addressed. We recommend that IT security staff approach ICS security by understanding the unique requirements these systems have and why they were set up that way. With that in mind, IT security staff should work with OT engineers to properly account for key systems, identify various dependencies such as OS compatibility and up-time requirements, and learn the process and operational practices to come up with a suitable cybersecurity strategy to properly protect these important systems.

Recommendations

Here are some recommendations for securing ICS endpoints:

- **Patch systems with security updates.** Though this is a tedious process, it is necessary for avoiding compromise; an example that illustrates this is how the Eternal Blue vulnerability was exploited initially by advanced zero-day malware, and then later on by commoditized Equation group tools installing coinminers. Once an exploit is out, it gradually gets assimilated into the attacker's playbooks, so it is important to patch.
- **Implement micro-segmentation in the network or use virtual patching technologies.** If patching is not an option, micro-segmentation enhances security by restricting network access and communications to the necessary devices.
- **Restrict network shares and enforce strong username and password combinations.** These can prevent unauthorized access through credential bruteforce.
- **Use Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).** These systems can flag possible network anomalies, detect malicious traffic, and help with device visibility. They can also help in profiling device-to-device communication, establishing a network traffic baseline, and address malicious network activities. Having a traffic baseline and profile of device-to-device communication makes it easier to identify network traffic anomalies later on.
- **Install antimalware solutions.** Antimalware solutions can address legacy worms and viruses that can stay dormant in removable drives and air-gapped systems. For ICS endpoints in air-gapped environments that do not have security software installed, or where security software cannot be updated because of the lack of internet connection, use standalone malware scanning tools that can scan and check for the presence of malware.
- **Set up USB scanning kiosks.** These stations can scan for malware from removable drives used to transfer data in between air-gapped endpoints.
- **Apply the principle of least privilege.** OT network administrators and operators should realize that an operator might control an ICS, but that does not mean the operator needs administrator privileges for the computer on which the ICS is running. Apply the principle of least privilege to the ICS such that an operator is allowed to use the system, but only an administrator can install software or make system modifications on the endpoint.

- **Consider regional differences in security awareness and implementation.** This is important to consider especially for multinational companies that might have facilities, partners, or subsidiaries in different locations around the world. Ideally, the same level of security is implemented whether the facility is in a relatively security-conscious culture or a less conscious one.
- **Identify and audit systems with low-risk tolerance.** Grayware can introduce unnecessary traffic or software that might interfere with the ICS. Depending on the risk tolerance the presence of grayware may or may not be tolerated. Identify and audit systems with low-risk tolerance to make sure only known and authorized software is used to mitigate risks.

Ransomware adversely impacts industrial systems, affecting visibility and control of industrial processes and disrupting operations. Post-intrusion ransomware is commonly the end product of an existing compromise, not the cause of it, and if ransomware is found in ICS endpoints, it means the access to such system is poorly secured or the network is fully compromised. To address this, we recommend the following:

- **Use a safelist or “allow list.”** For certain ICSs dedicated to specific functions, it might be appropriate to have a list that can enforce what software is allowed to run.
- **Conduct incident response and network sweeping for indicators of compromise (IoCs).** Post-intrusion ransomware groups use various tools and compromised accounts for access and lateral movement. By conducting comprehensive incident response and network sweep, security teams can determine the extent of the intrusion and the security weaknesses that were abused and come up with a robust security strategy based on the incident.

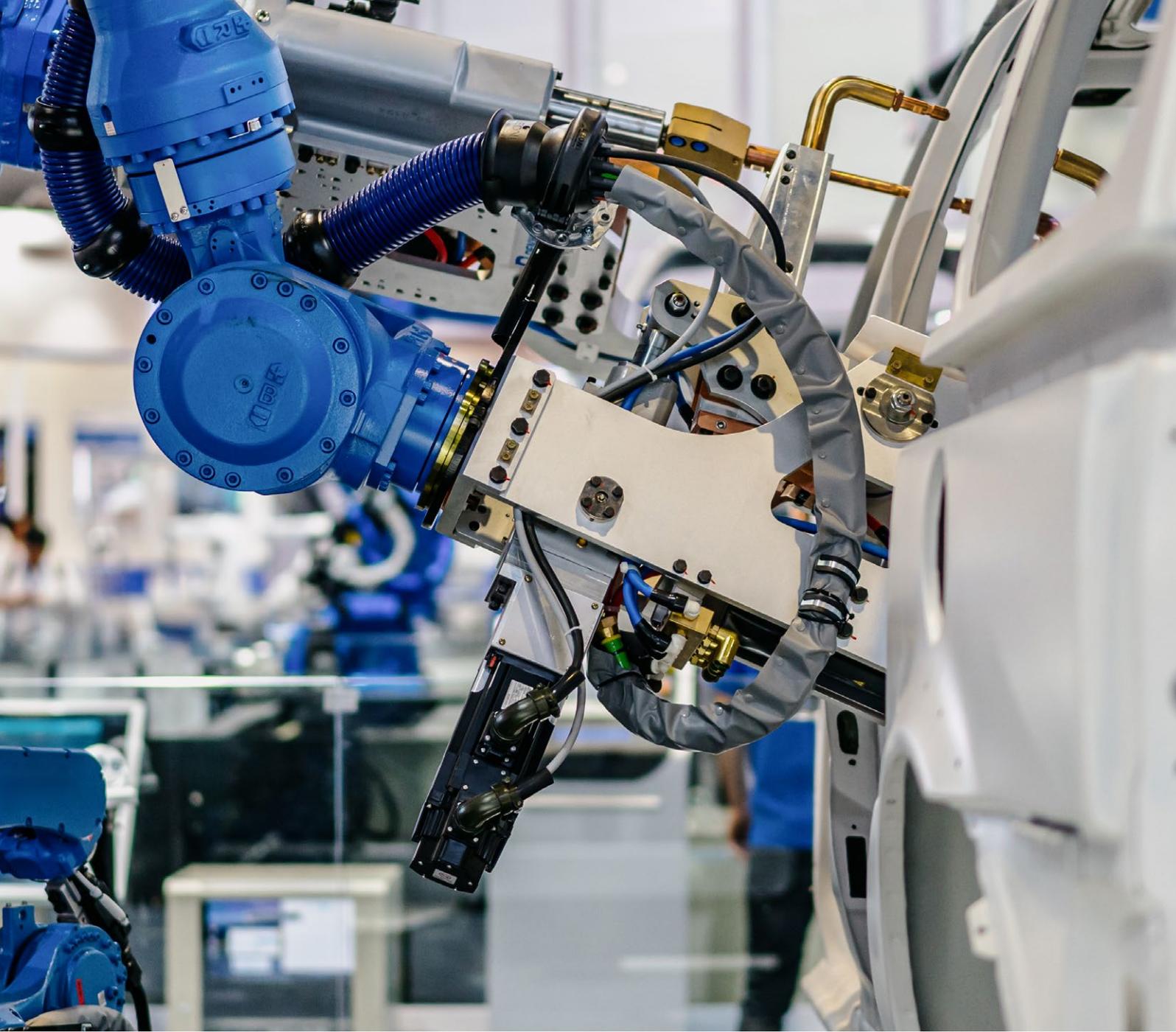
Indicators of Compromise

Conficker detections

SHA-256	Trend Micro
b2dcad48745325f3176483d698bb544339a052dd	WORM_DOWNAD.EZ
10256bbabf705c32a6ffc2bae5fe78518e722bab	WORM_DOWNAD.AD
5d6e19afa9ea3855a6812a9c28c56019144d672b	
77273bedd01886bc02c27a4b5c7da9d9428256d6	
ffb640274458c125f648b2b9f493a6de61af6329	
ee7276daf5962a3cc58ce87d1ce094d59de0256	
2b8964703209a0bc9606a7d08de3f0d0d2465be9	
7f91223d5e0d6c18ea0214b9dc731ce0739087f2	
c3d4becb6dbf94e948f7a3a81a73507d99a762b4	
85ae9c4e1d513d0f0ed7556c2d51791d7de4e7c0	
0d90356ee974ef47cbaa990c9086a8728e53874f	
71156637cebee20d1b227a591c6819bfe48d12c5	
0a175d05f2803a25d5b8069cdd40c7794743a23b	

References

- 1 Cedric Pernet, Vladimir Kropotov, and Fyodor Yarochkin. (June 13, 2019). *Trend Micro*. “Advanced Targeted Attack Tools Found Being Used to Distribute Cryptocurrency Miners.” Accessed on May 14, 2021, at <https://blog.trendmicro.com/trendlabs-security-intelligence/advanced-targeted-attack-tools-used-to-distribute-cryptocurrency-miners/>.
- 2 Viet Nam News. (March 18, 2019). *Viet Nam News*. “Internet users warned of ransomware attacks.” Accessed on May 14, 2021, at <https://vietnamnews.vn/society/507280/internet-users-warned-of-ransomware-attacks.html>.
- 3 Catalin Cimpanu. (Aug. 3, 2020). *ZDNet*. “GandCrab ransomware distributor arrested in Belarus.” Accessed on May 14, 2021, at <https://www.zdnet.com/article/gandcrab-ransomware-distributor-arrested-in-belarus/>.
- 4 Ryan Flores. (Dec. 01, 2020). *Trend Micro Research*. “The Impact of Modern Ransomware on Manufacturing Networks.” Accessed on May 14, 2021, at https://www.trendmicro.com/en_us/research/20/1/the-impact-of-modern-ransomware-on-manufacturing-networks.html.
- 5 Stephen Hilt, Federico Maggi, Charles Perine, Lord Remorin, Martin Rösler, and Rainer Vosseler. (Jan. 21, 2020). *Trend Micro Security News*. “Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats.” Accessed on May 14, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot>.
- 6 Ryan Flores. (Dec. 01, 2020). *Trend Micro Research*. “The Impact of Modern Ransomware on Manufacturing Networks.” Accessed on May 14, 2021, at https://www.trendmicro.com/en_us/research/20/1/the-impact-of-modern-ransomware-on-manufacturing-networks.html.
- 7 Jon Clay. (May 10, 2021). *Trend Micro Research*. “Tips to avoid the new wave of ransomware attacks.” Accessed on May 14, 2021, at https://www.trendmicro.com/en_us/research/21/e/tips-to-avoid-new-wave-ransomware-attacks.html.
- 8 Chaim Gartenberg. (April 21, 2021). *The Verge*. “Apple targeted in \$50 million ransomware attack resulting in unprecedented schematic leaks.” Accessed on May 14, 2021, at <https://www.theverge.com/2021/4/21/22396283/apple-schematics-leak-ransomware-quanta-supplier-leak>.
- 9 Stephen Hilt, Federico Maggi, Charles Perine, Lord Remorin, Martin Rösler, and Rainer Vosseler. (Jan. 21, 2020). *Trend Micro Security News*. “Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats.” Accessed on May 14, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot>.
- 10 Matsukawa Bakuei, Ryan Flores, Vladimir Kropotov, and Fyodor Yarochkin. (April 3, 2019). *Trend Micro Security News*. “Threats to Manufacturing Environments in the Era of Industry 4.0.” Accessed on May 14, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments?_ga=2.209525010.1874680133.1621125958-1328426616.1593403903.
- 11 Microsoft. (October 23, 2008). *Microsoft*. “Microsoft Security Bulletin MS08-067 - Critical.” Accessed on May 14, 2021, at <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>.
- 12 Dan Swincoe. (Aug 5, 2020). *CSO*. “What is a dictionary attack? And how you can easily stop them.” Accessed on May 14, 2021, at <https://www.csoonline.com/article/3568794/what-is-a-dictionary-attack-and-how-you-can-easily-stop-them.html>.
- 13 Danielle Veluz. (Oct. 1, 2010). *Trend Micro Threat Encyclopedia*. “STUXNET Malware Targets SCADA Systems.” Accessed on May 14, 2021, at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems>.
- 14 Magno Logan, Erika Mendoza, Ryan Maglaque, and Nikko Tamaña. (February 3, 2021). *Trend Micro*. The State of Ransomware: 2020’s Catch-22. Accessed on May 14, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22>.
- 15 Trend Micro. (March 18, 2020). *Trend Micro Security News*. “The IIoT Threat Landscape: Securing Connected Industries.” Accessed on May 14, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-iiot-threat-landscape-securing-connected-industries>.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

