



Securing Smart Factories

Threats to Manufacturing Environments in the Era of Industry 4.0

Matsukawa Bakuei, Ryan Flores, Vladimir Kropotov, and 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,
Vladimir Kropotov, and Fyodor Yarochnik**

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963-2017)

Contents

4

1. Introduction

8

2. IT Network Threats

17

3. OT Network Threats

24

4. IP Threats

30

5. Underground Activities Related to the Industrial and Manufacturing Sectors

32

6. Consequences of Security Breaches

34

7. Security Recommendations

37

8. Conclusion

A woman with blonde hair, wearing a yellow safety vest over a dark blue shirt, is seated at a workstation in a factory. She is looking at a computer monitor which displays a technical drawing of a mechanical part. Her right hand is on a computer mouse. In the background, a man with glasses is partially visible, also looking at the screen. The background is slightly blurred, showing industrial equipment and bright overhead lights.

The fourth industrial revolution, dubbed Industry 4.0, introduces the use of cyber-physical systems (CPSs) in production processes, where the industrial internet of things (IIoT), machine learning, and big data and analytics play key roles. Adopters of Industry 4.0 push for a more connected and efficient production that in turn boosts their competitiveness in the market. The interconnected nature of Industry 4.0 drives digital transformation in manufacturing, as information technology (IT), operational technology (OT), and intellectual property (IP) all converge to support the realization of so-called “smart factories.”

Apart from introducing opportunities, however, Industry 4.0 comes with its challenges. Integrating the organization’s IT infrastructure with the OT and IP sides of the business means that the attack surface increases significantly. Threat actors will find more weak points to break the security of the production. Attacks designed to target industrial control systems (ICSs), in particular, pose threats to production facilities.

Organizations are now faced with the challenge of upgrading measures to protect IT, OT, and IP against any weak link an adversary may take advantage of. Unsupported operating systems, unpatched vulnerabilities, and exposed systems risk both physical and digital manufacturing components. Compromised systems and exploited flaws could lead to data leaks, financial losses, and production downtime.

In this paper, we take a look at the unique threat and risk landscape of the manufacturing industry, underscore the challenges brought about by the move to Industry 4.0, and recommend measures and best practices for securely reaping the benefits of connected production. We also reiterate that securing the manufacturing industry requires regular risk assessments and a resilient cybersecurity framework that is able to detect, respond to, and protect against a variety of security holes.

1. Introduction

The manufacturing industry is an important economic driver in most countries. For developing countries, industrialization is a key economic strategy where they try to entice multinational companies to set up local manufacturing facilities through cheap labor, tax breaks, and provision of logistics and infrastructure. In return, a new manufacturing facility provides jobs and stirs economic activity crucial for the economic growth of a developing nation.

Developed countries, meanwhile, are often investing in the development of technology companies that focus on research of high-value products. Of course, they intend to keep their competitive edge in the area of high technology and high-value production, which is why they are looking into the competitive advantages touted by the Industry 4.0 concept. The manufacturing giant China, for example, is faced with the reality that its wages have been increasing and industrial robotics has been presented as a better option for automation and offsetting labor costs.¹ In some developed countries, Industry 4.0 has been declared as part of their long-term economic strategies.

Country	Strategy
China	Made in China 2025 ²
Germany	Industrie 4.0 ³
India	Digital India ⁴
Japan	Society 5.0 ⁵
Russia	4.0 RU ⁶
United States	Industrial Internet Consortium ⁷

Table 1. Some country initiatives on transforming industries

Just as the internet of things (IoT) connects devices and systems through interoperability,⁸ Industry 4.0 ushers in the use of the IoT for automation and data exchange in manufacturing, as embodied by a smart factory.⁹ The term *Industry 4.0* was coined by the German government in 2011 to describe the convergence and benefits of cyber-physical systems (CPSs) in the industry.¹⁰ In the preceding revolution, Industry 3.0, the use of automation and computers were limited to siloed implementations. It was also not

necessary for the production machines to communicate with other pieces of equipment or sync with other systems such as for order, procurement, and production. Industry 4.0 requires the interconnection of these systems and recognizes its benefits: increased productivity and efficiency, on-demand manufacturing, and improved data retention for compliance.

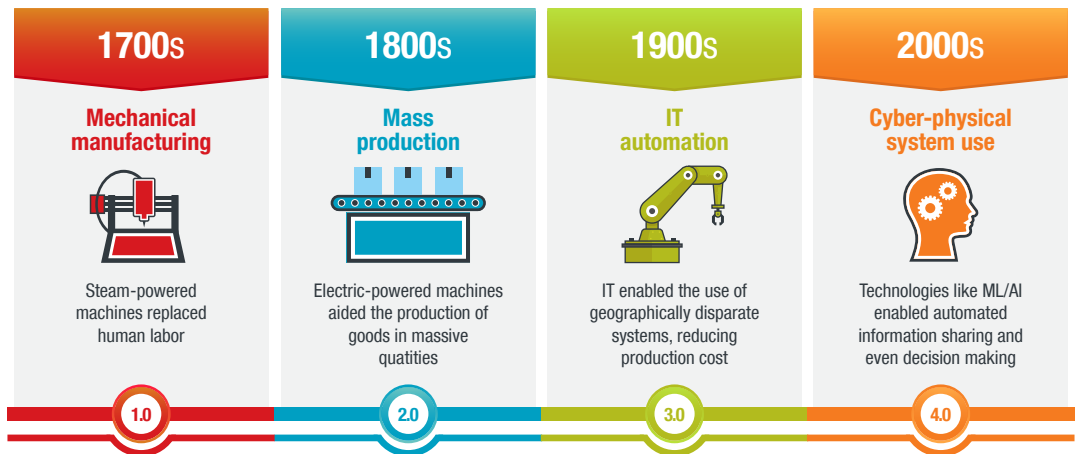


Figure 1. From Industry 1.0 to Industry 4.0

Industry 4.0 is attractive to top technology companies, as they often innovate not only on their products but also on the manufacturing process itself — introducing best practices on quality control and developing more efficient processes in vendor, order, and supply chain management for original equipment manufacturers (OEMs) of materials or components. The interconnection of various management and production systems is the key characteristic of Industry 4.0.

However, moving to Industry 4.0 drastically alters the threat risk model of a manufacturing company. The operational technology (OT) network, previously isolated, now needs to be connected to the information technology (IT) network, which introduces various security challenges such as support for old equipment, software updates, and patching. Moreover, network latency and CPU utilization must remain within acceptable limits so as to not be detrimental to the manufacturing process. Intellectual property (IP), a source of competitive advantage, also needs to be secured. The need for transferring data between the IT and OT networks — as well as sharing information with select external partners, suppliers, or vendors — requires a delicate balance between securing the networks to thwart espionage and enforcing proper restrictions and access management on IP assets.

The Manufacturing Industry: Where IT, OT, and IP Intersect

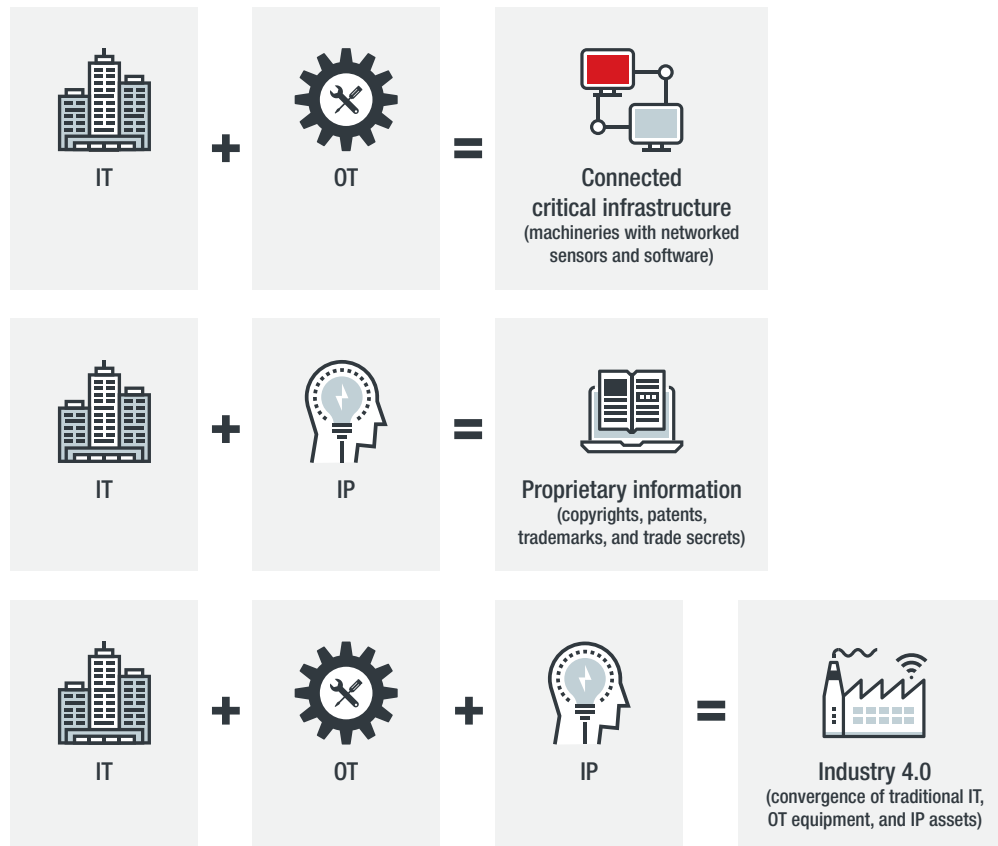


Figure 2. Convergence of information and networks in manufacturing

The manufacturing industry is an interesting convergence of OT (the industrial network), IT (the enterprise network), and IP (intellectual property). Most critical infrastructures, such as infrastructures responsible for the provision of energy or water, are a mix of OT and IT only, while some advanced research facilities, such as universities, have IT and IP only. But the manufacturing industry combines all three, thereby creating a unique set of challenges. This is especially true now as the move to Industry 4.0 requires the convergence of IT and OT networks,¹¹ centralization and specialization of manufacturing, and the integration of protocols and devices that were not designed to be part of a TCP/IP (Transmission Control Protocol/Internet Protocol) world.

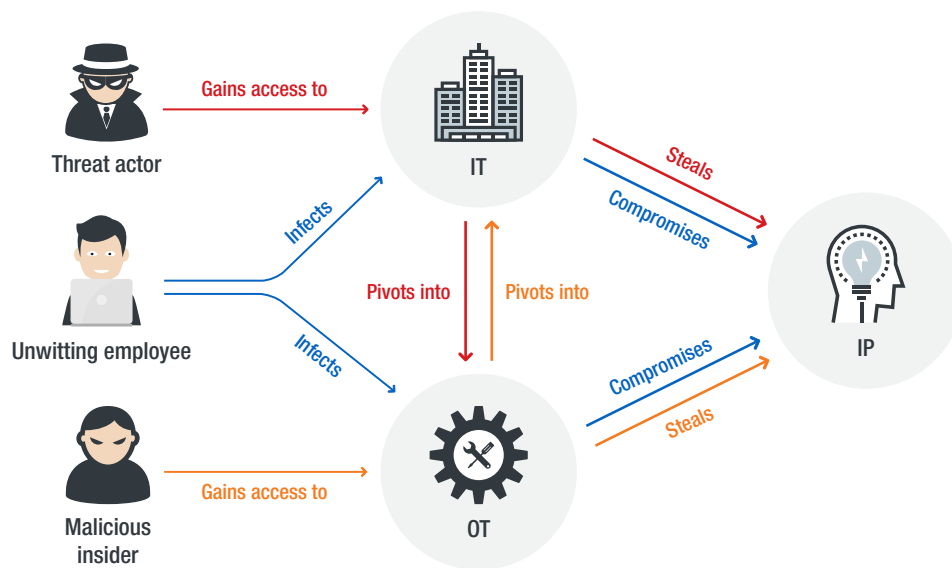


Figure 3. How threats can figure into the IT, OT, and IP convergence

Manufacturing equipment has long life cycles, with heavy machinery lasting, on average, anywhere from 26 to 34 years, while computers and related equipment have an average lifetime of around nine years before replacement or decommissioning.¹² As a result, Industry 4.0 adoption — where various pieces of equipment and systems in the production line are able to communicate with one another — takes a few years, even a decade, to be realized. In the meantime, we see an industry that is slowly moving toward Industry 4.0 by replacing equipment piece by piece, whether as part of the normal equipment upgrade life cycle or as part of a new plant construction. We see an industry that is at a crossroads — moving away from the current status, yet not fully into Industry 4.0. Consequently, such an intermediate state poses its own set of threats and risks.

2. IT Network Threats

The IT networks of manufacturing companies are structured and organized just like any other network. However, certain operational practices and network configurations make the manufacturing networks more susceptible to certain types of malware threats. As we discuss later with our data, this is especially true in manufacturing network environments, where a single failure from a software update, an incompatibility error, or a simple system restart could lead to more significant failures in a production process and cause financial loss. The software update and patching cycle is not as strictly followed in the manufacturing industry as in other industries. In addition, it is commonly believed — yet is not necessarily true — that manufacturing networks are isolated, and thus safe from external threats.

Using data from the Trend Micro™ Smart Protection Network™ infrastructure, we examined the detection logs in the manufacturing industry and compared them to detections in other industries, such as energy, education, healthcare, and government. In doing so, we aimed to demonstrate that networks in the manufacturing industry are exposed to external threats, like those in any other industry. Moreover, we also looked into several security weaknesses that serve as entry points for adversaries targeting the manufacturing industry.

It is important to note that the IT network in the manufacturing sector serves as a vital clearinghouse in the adoption of Industry 4.0. The IT network not only serves as the network where employees check emails, create designs, and handle engineering tasks; it is also the network where production data is reported, such as order requests on one side and delivery and logistics on the other. Thus, it is important to monitor malware threats in a manufacturing IT network, as adversaries can sabotage the entire pipeline if they gain a foothold in critical servers, use the IT network to pivot into the OT network, or steal IP residing in file servers, network shares, or backup drives.

2.1 Threat Exposure of Manufacturing Networks Due to Longer Equipment Life Cycles

2.1.1 Prevalent Use of Windows XP

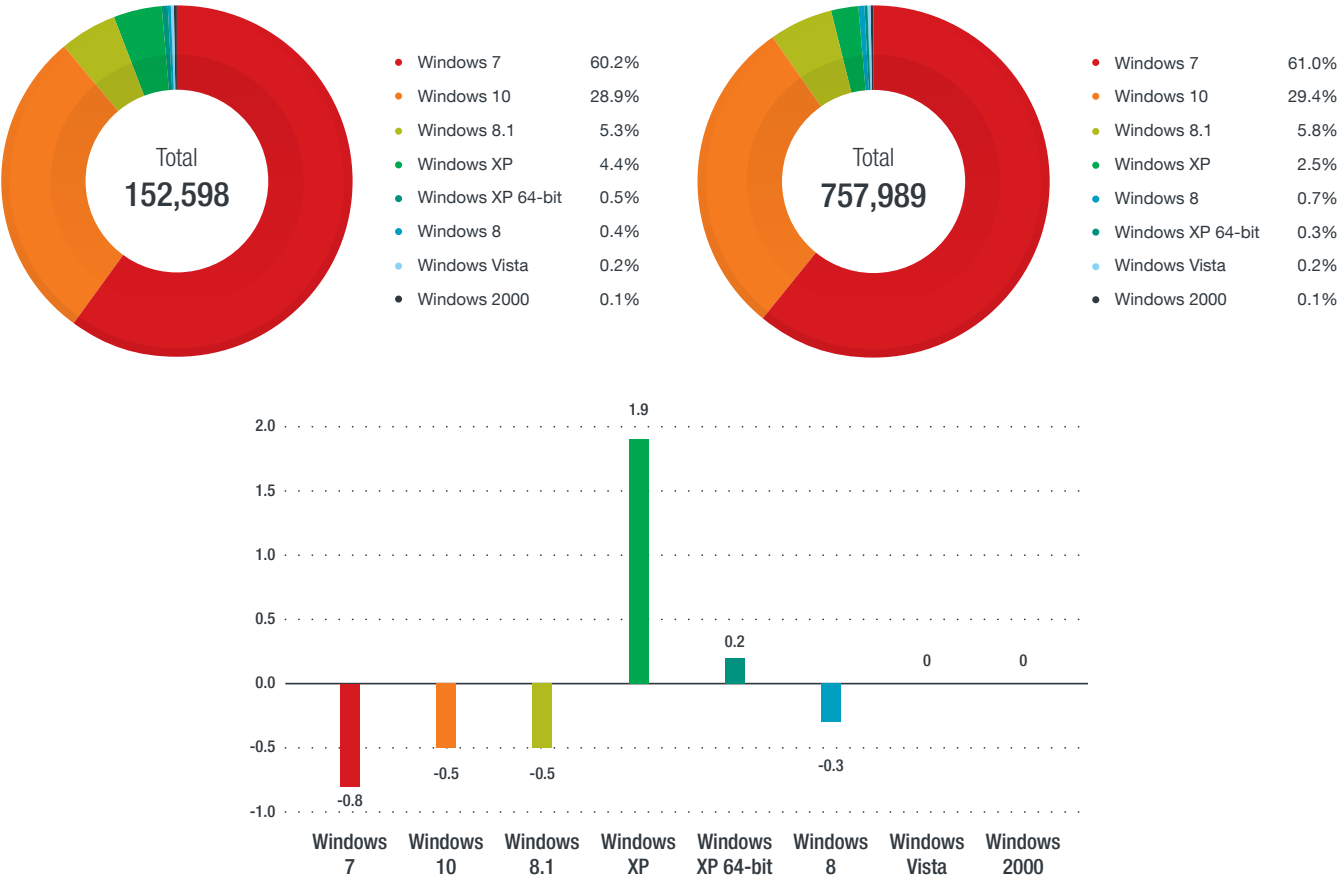


Figure 4. Top operating systems in the manufacturing industry (top left) and in other industries (top right), and percentage point differences between distribution of operating systems in the manufacturing industry and that in other industries (bottom), based on data from the Trend Micro™ Smart Protection Network™ infrastructure for the period from July to December 2018

Comparing the distribution of operating systems in the manufacturing industry with that in other industries, we see that the percentage point differences are highest for Microsoft® Windows® XP and Windows XP 64-bit edition. This suggests that the use of these operating systems, support for which ended in 2014,¹³ is more pronounced in the manufacturing industry than in other industries. This situation is most likely caused by a combination of a “do not touch a working system” mentality and the long replacement cycle in hardware and software equipment. It is frequently seen in the manufacturing sector that the software

components and drivers that support specialized equipment may not be compatible with more recent operating systems. Because of the long life cycles of specialized equipment, the functional hardware may be considered obsolete by its vendor or may have reached end of support. In other cases, some systems or software may be left unsupported when a vendor merges with or acquires another vendor. In these instances, the software used to operate the hardware may no longer be supported, maintained, and updated, thus forcing equipment operators to use old operating systems to be able to continue running the equipment.

2.1.2 Pervasiveness of Network Worms

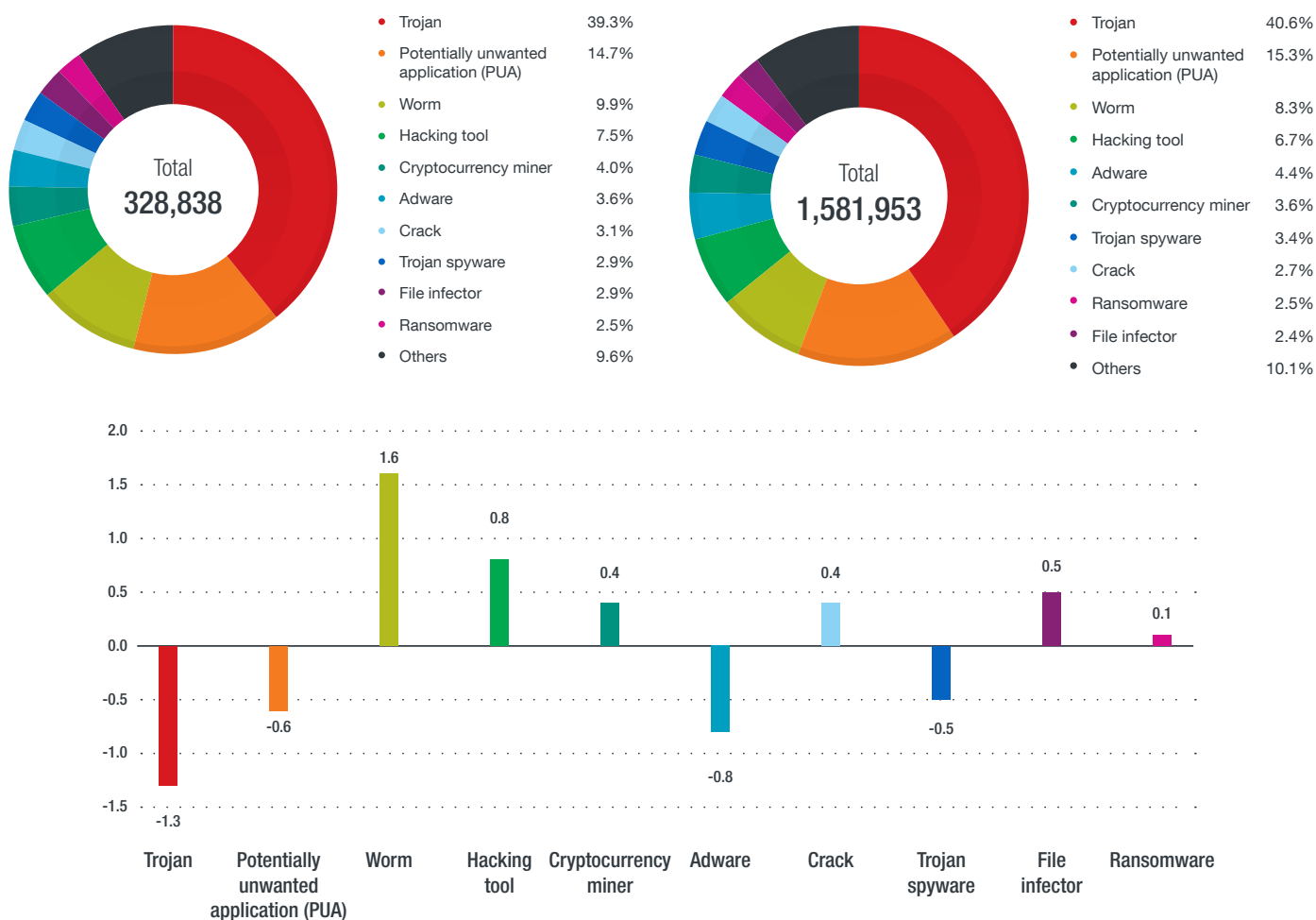


Figure 5. Top malware types in the manufacturing industry (top left) and in other industries (top right), and percentage point differences between distribution of malware types in the manufacturing industry and that in other industries (bottom), based on data from the Trend Micro Smart Protection Network infrastructure for the period from July to December 2018

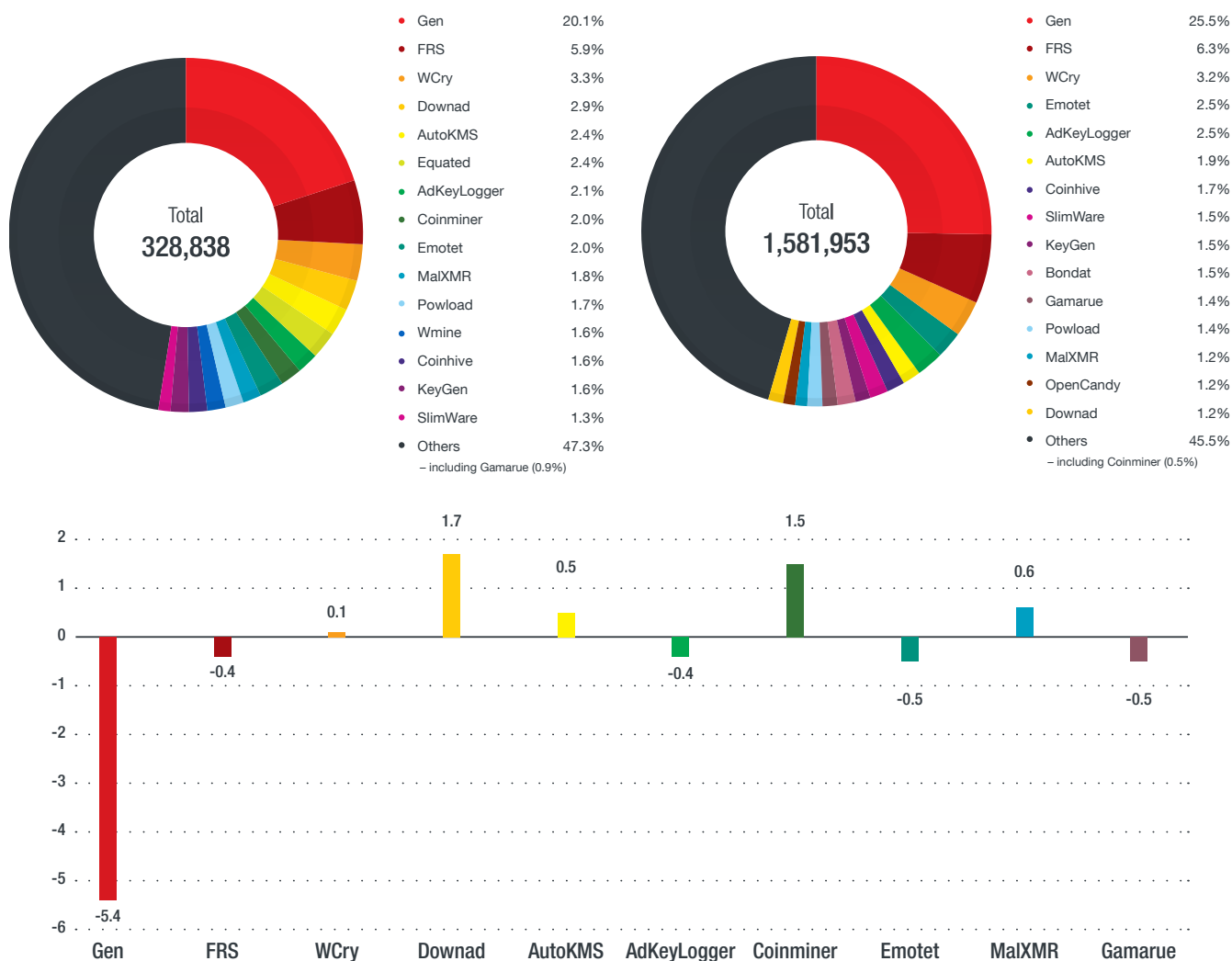


Figure 6. Top malware families in the manufacturing industry (top left) and in other industries (top right), and percentage point differences between distribution of malware families in the manufacturing industry and that in other industries (bottom), based on data from the Trend Micro Smart Protection Network infrastructure for the period from July to December 2018

One of the side effects of having old and unsupported operating systems in the manufacturing industry is the presence of a large number of unpatched vulnerabilities that could be exploited by old variants of network malware. It is no surprise that detections of such malware families as Downad (aka Conficker),¹⁴ WannaCry (WCry),¹⁵ and Gamarue (Andromeda)¹⁶ are relatively high on machines used in manufacturing environments. Detections of worms in general and Downad in particular are significantly prevalent in the manufacturing industry.

Downad is a 10-year-old worm whose primary propagation method is the exploitation of an old vulnerability in Windows systems; it also propagates through removable drives (USB drives) and network shares. Although it first appeared in 2008, Downad continues to be a considerable threat to this day. In fact, we have seen it become one of the top malware infectors for both enterprises and small and medium-sized businesses (SMBs). Downad thrives in major industries, particularly in manufacturing, because of how

upgrading systems could be a choke point for business continuity. The malware has the greatest impact on legacy systems, where unsupported and unpatched systems still play a regular role in an organization’s network.

As for the WannaCry detections, interestingly, a large number of older versions of Windows XP are likely not infected by the ransomware because the EternalBlue exploit it uses would not work on these versions.

2.1.3 Autorun Detections

One of the common propagation methods of Downad and other USB worms is *autorun.inf* abuse, by which they can automatically execute whenever an infected removable device is plugged in. Looking at the number of devices that detected *autorun.inf*, we observe that the manufacturing industry has significantly higher detections than other industries. This reflects the common practice in the industry of using USB drives to copy and transfer information between computers and networks (the IT and the OT) in a manufacturing environment. It is important to note that the famous Stuxnet malware, which was designed to target a nuclear facility, was propagated using removable USB media, although the malware itself exploited a vulnerability in parsing shortcuts.¹⁷ For manufacturing, we can say that the industry is more susceptible to USB-based malware propagation than any other industry, based on the significantly higher detection of malicious *autorun.inf*.

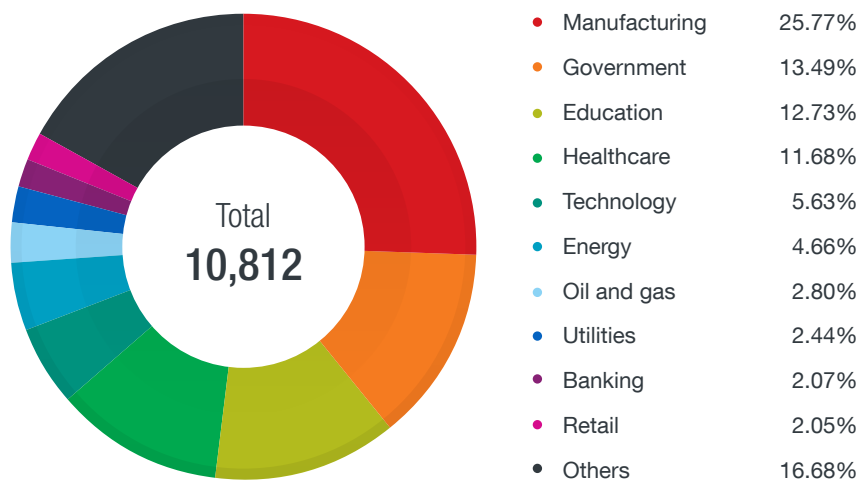


Figure 7. Detections of *autorun.inf* across industries, with manufacturing having the highest, based on data from the Trend Micro Smart Protection Network infrastructure for the period from July to December 2018

2.2 Targeted and Opportunistic Campaigns Against the Manufacturing Industry

Analysis of recent infections provides insights on how the unique network setup and architecture of industrial or manufacturing environments can shape their threat landscape. Manufacturing, like any other industry, suffers from both targeted campaigns and opportunistic hacking incidents. We found a number of targeted malware infections and opportunistic malware detections in observed environments.

2.2.1 PlugX for Targeted Attacks

One of the recent incidents involving the PlugX malware attracted our attention. PlugX is an advanced remote access tool (RAT) that is commonly used in targeted attacks for espionage or information exfiltration.¹⁸ So when we identified a breach of a Chinese manufacturing company with the PlugX malware family, it appeared to us as unusual. There were several surprising facts about this series of incidents. For one thing, we rarely observe PlugX campaigns inside China. The hacker groups that use PlugX commonly focus on other countries and often infiltrate government and technology sectors. In this group of incidents, however, we identified a number of PlugX infections in China that seemed to be targeting the manufacturing sector.

A common use of a PlugX backdoor is for industrial espionage, and we expected to identify this kind of activity within a compromised network. The second surprising part was not the malware itself, but the hacker activities on the compromised network. The attacker apparently was not interested in any data on their targets. Instead, the attacker exhibited a different objective.

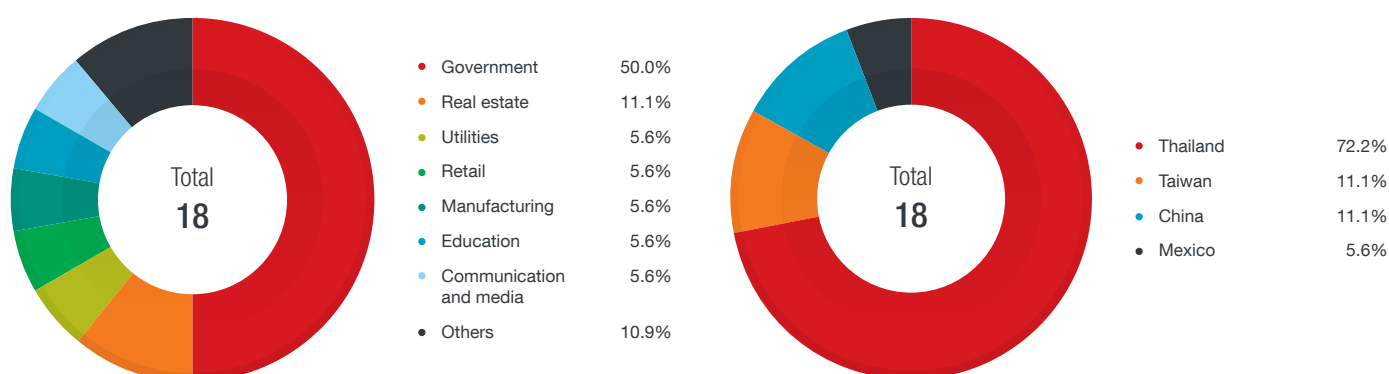


Figure 8. PlugX detections by industry (left) and by country (right), based on data from the Trend Micro Smart Protection Network infrastructure for the period from July to December 2018

Starting from September 2017, the attacker compromised several manufacturing companies and deployed the PlugX RAT on the compromised machines to secure remote access to these assets. Furthermore, this backdoor was used by the attacker to maintain remote persistence in compromised machines and facilitate lateral movement in the systems. In all cases, the initial breach took place through a vulnerable web service of a compromised organization. Once a machine was compromised, the attacker uploaded a PlugX bundle installer (named *demo.exe*) and a Mimikatz tool (named *ms32.exe*). The attacker used the same names for the files across different targets. The bundle installed PlugX as *iusb3mon.dll* and *iusb3mon.exe* binaries. The *iusb3mon.exe* binary was a validly signed binary and the attacker used a dynamic link library (DLL) search order hijacking vulnerability to make the binary load the RAT code.¹⁹ The Windows registry was modified to execute *iusb3mon.exe* on system startup. This is one of the common persistence mechanisms used by PlugX that is often used to bypass detection when only non-signed files executed at startup are checked.

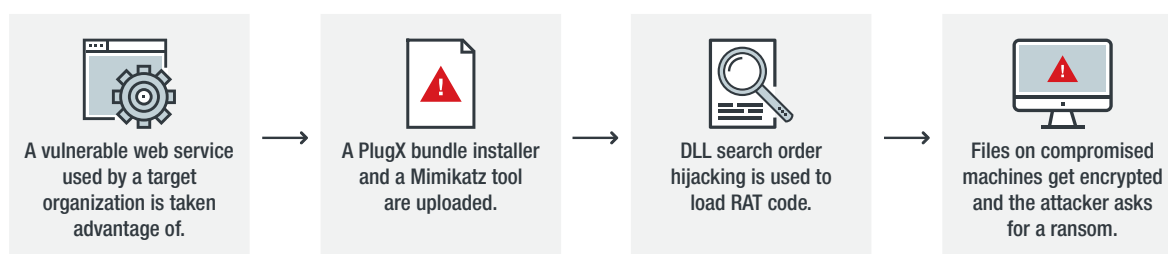


Figure 9. Visualization of a PlugX infection incident in manufacturing

The attacker also used Mimikatz to collect credentials and move laterally within the systems.²⁰ (Mimikatz had previously been used with other hacking tools and cryptocurrency-mining malware to collect system credentials.) Each compromised machine also had the PlugX RAT deployed. As the final stage, the attacker encrypted the files on the compromised machines and left a note to the system owner asking for a ransom.

While we were looking into this incident, researchers from Tencent's security team reported in a blog post an incident that featured very similar findings.²¹ The amount of ransom requested in this case was 9.5 bitcoins (at the time equivalent to about US\$76,000²²).

We could not verify whether the ransom was paid to the attacker or not. But in each instance of the breach, the attacker targeted companies within the manufacturing sector in China. We continued to monitor compromised machines and noticed that aside from deploying the ransomware components, the attacker also deployed and executed cryptocurrency-mining software on the compromised machines. To our surprise, we observed that the cryptocurrency miner remained on compromised systems for quite a prolonged period before it was detected and removed by the system owners. While the compromised machines did not possess significant computing power, the attacker likely chose to deploy cryptocurrency-

mining software as a less risky way to monetize their access to the compromised assets — possibly after realizing that their ransom demands had not been met.

However, as can be seen in the detections indicated in Figure 6, cryptocurrency miners are not uncommon on manufacturing networks, coming in second after Downad in terms of prevalence relative to other industries. Cryptocurrency miners also have significantly higher infection rates in manufacturing than in other sectors.

The aforementioned series of incidents shows instances of compromise in the manufacturing industry where cybercriminals run cryptocurrency-mining software when other means of monetizing access to compromised assets have been exhausted. Knowing that old computer hardware is common in the industry, organizations should be concerned that their systems may be used for cryptocurrency mining. A simple delay or failure in systems may lead to considerable consequences.

Another threat the manufacturing industry should be on the lookout for is ransomware attacks that can cause far more damage than in other industries if the manufacturing line is affected. This notably happened to at least a couple of car manufacturers during the WannaCry ransomware outbreak in May 2017,²³ and more recently to a well-known chipmaker, which had to shut down several of its factories after being infected by a new variant of WannaCry in August 2018.²⁴ The ransomware LockerGoga also recently made headlines for hitting a Norwegian aluminum manufacturer and forcing plants to switch to manual operations.²⁵ In the case of ransomware, not only could the manufacturing industry be hit by the cost of data recovery, but the downtime in a manufacturing facility could result in huge financial losses as well.

2.2.2 Dormant Infections in Networks

Instances of “commodity” ransomware also commonly appear in manufacturing networks. It is assumed that manufacturing networks are isolated with no connection to the internet. However, this is not entirely the case. There are still channels that could be — and are often — used by malicious software to infiltrate isolated segments of the network. This could happen when an infected computer is connected to such a network or when isolation is not done properly. In general, incorrectly isolated networks create a fake sense of security, which makes the general security posture of the systems inside these networks not very high. After all, availability is a high priority in this industry, so functional (but outdated) systems are often not upgraded. This is because a security patch may cause problems with custom software that is run on such systems.

Isolated networks, therefore, are not entirely safe from internet worms. As noted earlier, the prevalence of Downad in networks shows that old malware strains can thrive in such environments. In fact, some of the malicious pieces of software can cause significant damage even after the malware has been publicly discovered and mitigated for quite some time.

For example, WannaCry had a “kill switch” domain feature, which might not behave as expected on an isolated network. For this ransomware, the domain was registered to ensure that the malware would no longer spread. However, in isolated networks, the ransomware would not be able to find the kill switch domain and infection would still propagate or cause damage.

There were a number of notable ransomware incidents in the manufacturing industry that exhibited these issues. The previously mentioned WannaCry outbreak, for instance, led to significant losses in several manufacturing companies. The amount of financial loss due to downtime caused by the outbreak also led to significant public attention.²⁶ Separately, a transmission plant was shut down due to a ransomware outbreak in August 2016.²⁷

There is another potential security impact of network isolation: Once infected, an isolated network could allow many types of malware to successfully propagate because they do not rely on internet access. Security tools such as endpoint security solutions would have limited capabilities due to their inability to frequently update signatures or make use of back-end network security. We often observe deployments of security products on isolated networks, where the software has not been updated for more than five years. Given the speed of evolution of network security threats, this essentially renders such software deployments useless.

Weaponized documents (e.g., design documents and office documents) could also have an impact on isolated networks when delivered through internal IT systems (e.g., by way of internal messaging, USB keys, or external storage). When these documents are opened on isolated networks, they can cause the same damage, and security tools may fail to detect these threats due to the same aforementioned shortcomings of endpoint security solutions in isolated networks.

In addition, execution of malware in isolated networks could trigger the nonstandard, and potentially destructive, behavior of malware, because the malware may wrongly assume that it is being executed in a sandboxed environment.²⁸

Manufacturing networks exhibit a unique characteristic of running systems that are significantly outdated compared to those used in other industries. A large number of dormant malware infections, which likely have been known for a long time, may be successfully detected and mitigated in more agile environments than manufacturing.

3. OT Network Threats

The move toward Industry 4.0 has the biggest impact on the connectivity of the OT network. Previously isolated and running its own protocols, the manufacturing network is being slowly integrated with the IT network for real-time visibility and control, and integration into various systems that make up the production line, supply chain, sales, and enterprise systems. Thus, computers and controllers in the manufacturing network are now exposed to a wider range of threats. This requires both IT administrators and OT engineers to work together to bring the security or protection of such systems up to speed without compromising any operational requirements.

In this section, we list three things IT administrators and OT engineers need to look into when securing manufacturing equipment and controllers: industrial control system (ICS) vulnerabilities, exposed systems due to network misconfigurations or poor design, and malware targeting ICSs.

3.1 ICS Vulnerabilities

Modern manufacturing equipment has human-machine interfaces (HMIs) that allow operators and engineers to monitor and control the equipment. Programmable logic controllers (PLCs) are used to program logic into several pieces of equipment, enabling them to take action based on certain conditions or thresholds as reported by other pieces of equipment or sensors. Furthermore, there are industrial-grade routers, hubs, and gateways that handle the networking in the manufacturing network.

Just like any normal system, these pieces of equipment and devices have vulnerabilities. According to vulnerability reports submitted to the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) as of September 2018, the number of vulnerabilities affecting manufacturing-related equipment jumped significantly in 2014 — a trend that continues to this day. (The ICS-CERT also collects vulnerability reports for healthcare equipment, but for the purpose of this paper, we included reports for industrial equipment used in manufacturing and heavy industries only.)

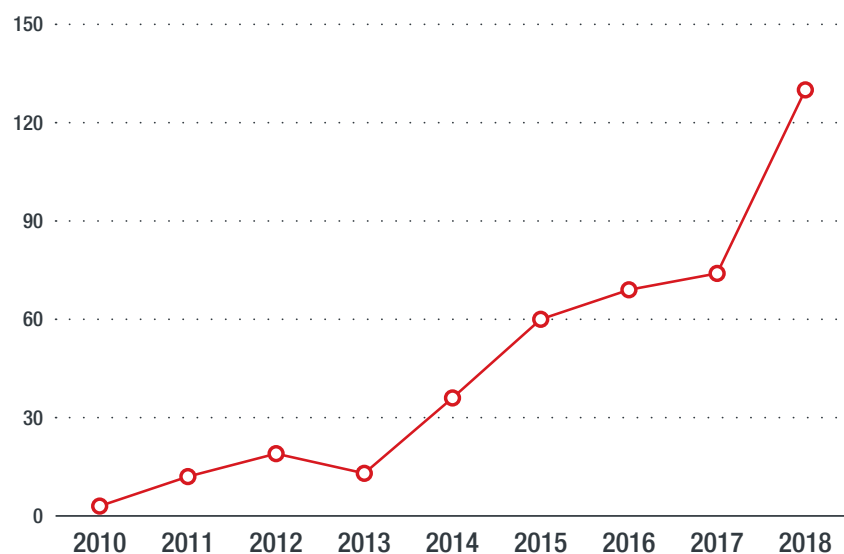


Figure 10. Trend of vulnerabilities affecting manufacturing-related equipment reported to the ICS-CERT

If we dig deeper in the reported vulnerabilities by vendor, we see that the ICS vendors Siemens, Rockwell Automation, and Schneider Electric top the list. This is not surprising since these vendors have a wide range of products and the highest market shares in this industry.

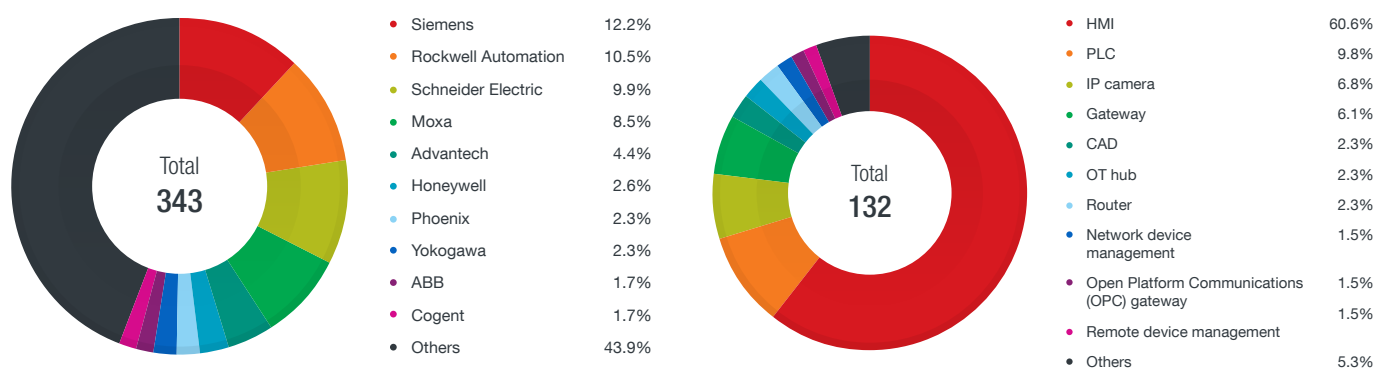


Figure 11. Vendor distribution of vulnerabilities reported to the ICS-CERT (left) and equipment type distribution of 132 ICS/SCADA-related exploits on ExploitDB (right)

Most of the publicly available exploits involve HMI vulnerabilities. Most HMIs are in effect applications, sometimes having web access, so “traditional” web exploits are applicable here. According to a study by Trend Micro’s Zero Day Initiative (ZDI) team, common security problems with HMIs involve memory corruption (stack- and heap-based buffer overflows and out-of-bounds read/write vulnerabilities), poor credential management (use of hard-coded passwords, storing passwords in recoverable format, and insufficiently protected credentials), and lack of authentication and unsecure defaults (clear text transmission, missing encryption, and unsafe ActiveX controls).²⁹

Having a vulnerability is one thing, but having an actual exploit against that vulnerability makes attacks much easier. Out of the 343 vulnerabilities related to ICSs and supervisory control and data acquisition (SCADA) systems reported to the ICS-CERT, there are 132 for which exploits can be found on ExploitDB, a database of publicly available exploits. This means that anyone, from penetration testers to cybercriminals, can use publicly available exploit code to attack parts of an ICS environment.

The presence of these systems and their vulnerabilities means that the OT network should have the same level of network protection as the IT network. The available exploits against HMIs, for example, can be flagged by intrusion detection products that support SCADA protocols. However, intrusion prevention systems (IPSs) are quite uncommon in ICS environments because of the complexity of network protocols and significant impact of false positives: An incorrectly blocked request in an ICS environment could lead to a failure in the in the CPS.

3.2 Publicly Exposed ICSs

In some cases, attackers do not need to exploit any vulnerability in order to control or sabotage a critical manufacturing machine or production line. We have seen several cases where an HMI is directly exposed to the internet, without authentication. This basically allows anyone to tamper with values and issue commands on manufacturing machinery if the HMI is not read-only. Some of these interfaces provide read-only access and are used for monitoring purposes only, while others are not. Any unauthorized tampering of such systems can result in production delays, product contamination, physical hazards, or destruction of equipment.

The risks to exposed critical infrastructures, specifically those in the energy and water industries, were identified in a report published by Trend Micro in 2018.³⁰ Cyberattacks against these industries could lead to supply disruption. For instance, operational disruption in a water facility could mean manipulated temperatures and supply of drinking water in an area. And power services to homes and businesses could be cut off by malicious actors.

Below are some examples of manufacturing machines we found using the IoT search engine Shodan during the course of this research.

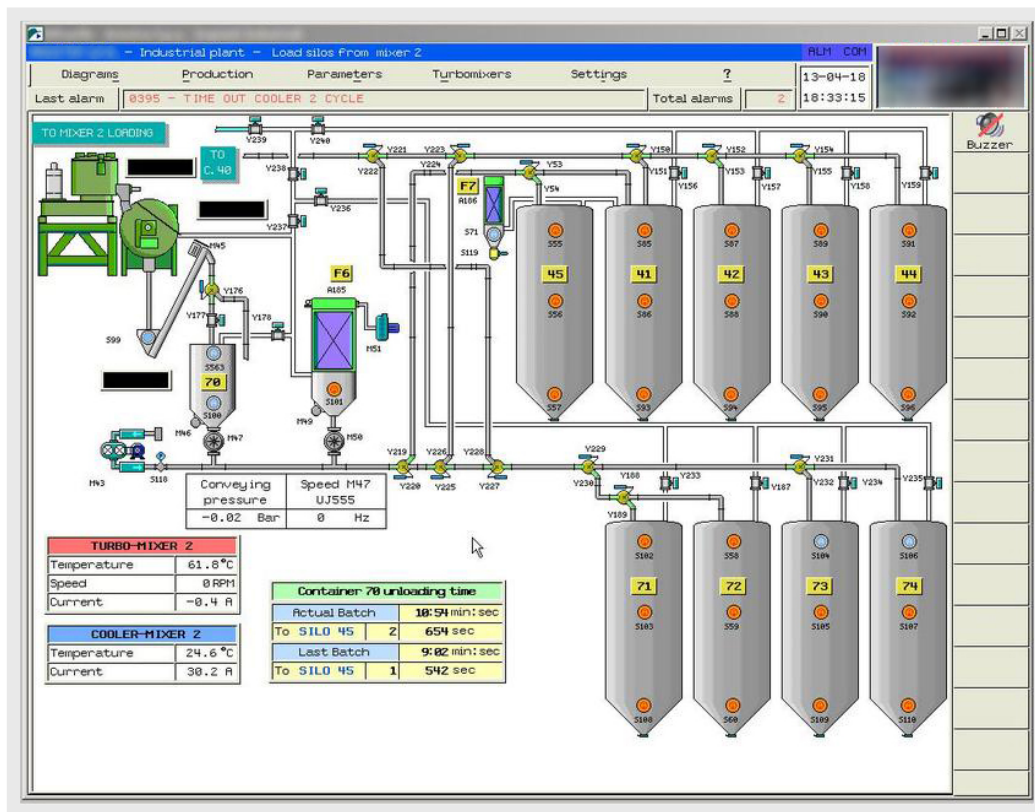


Figure 12. Monitor for mixers and their temperature and speed numbers

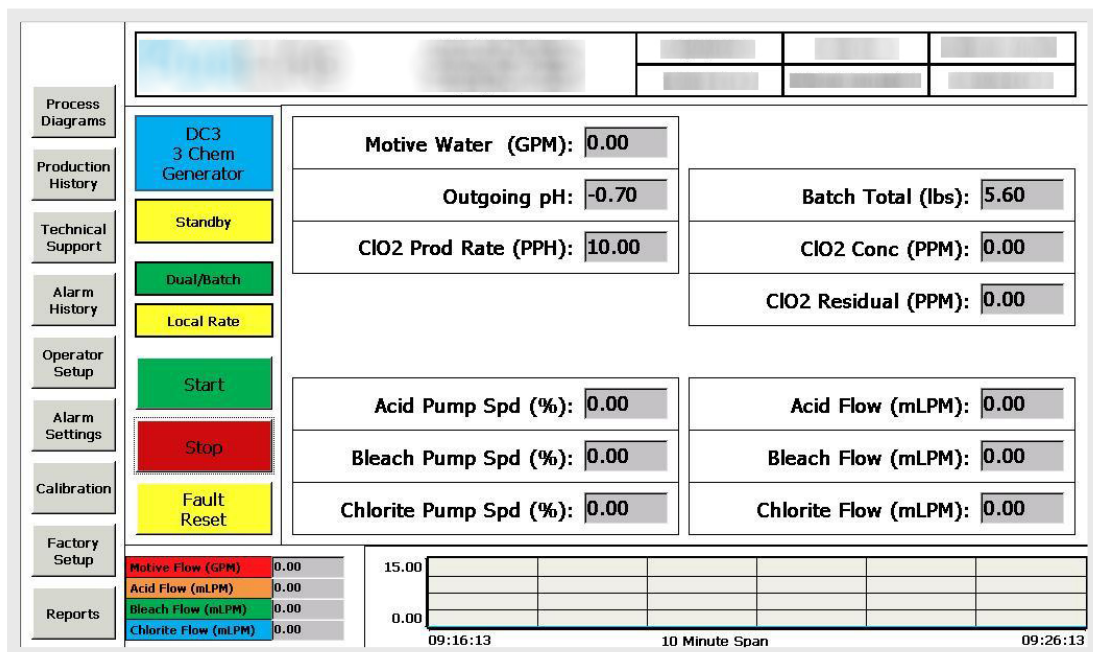


Figure 13. Menu showing readings from different subsystems, with accessible start, stop, and fault reset options

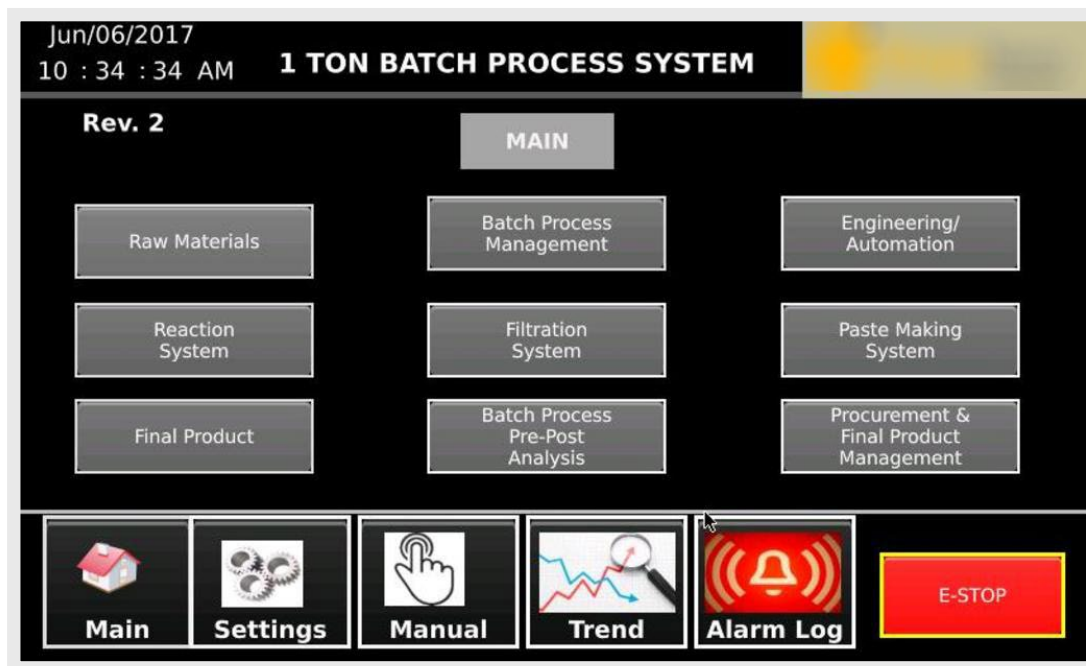
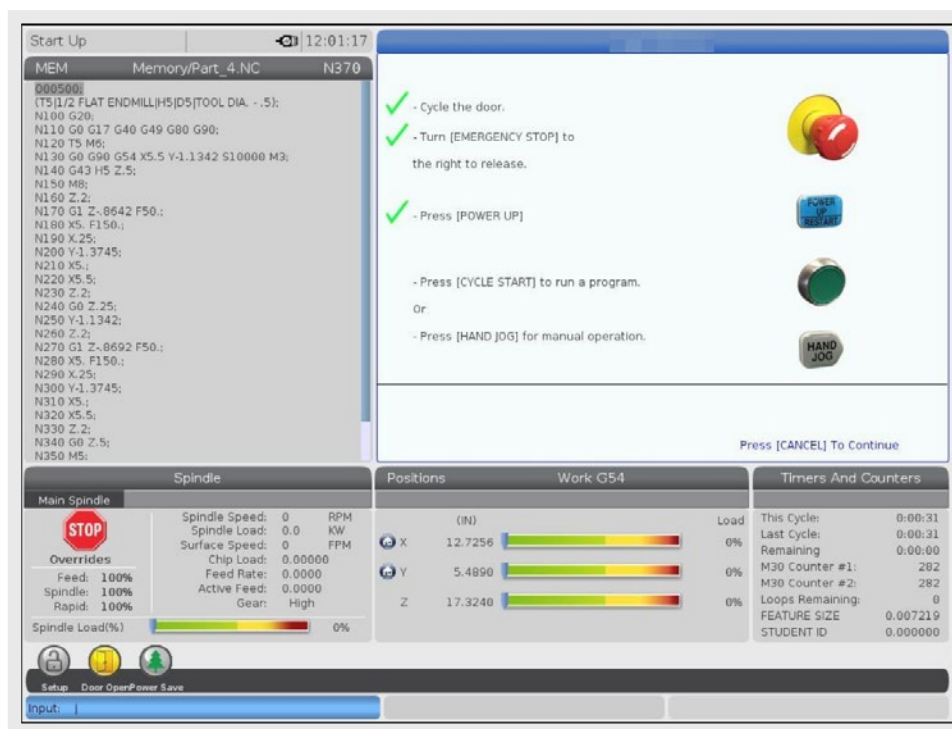


Figure 14. Overview page displaying a batch process system and emergency stop (e-stop) option



Figure 15. Exposed HMI for a bending tool



3.3 Malware Targeting ICSs

One of the goals of adversaries targeting the manufacturing industry is to gain access to ICSs for sabotage, control, or extortion. The increasing connectivity between OT and IT networks enables adversaries to pivot from a breach originating in the IT network to ICS devices in the OT network. Although uncommon, malware specifically designed to target ICSs has been seen before. In 2014, for instance, samples attributed to the Sandworm team was found to target GE Intelligent Platform's Cimplicity® HMI software,³¹ which is used in many manufacturing and industrial applications for monitoring and controlling ICSs.

Also in 2014, a variant of the Havex malware was seen to be capable of scanning for Open Platform Communications (OPC) servers.³² OPC servers are used to communicate with ICS devices by translating the ICS protocol into OPC, thereby enabling computers in the IT network to communicate with ICS devices. Havex's feature of scanning for OPC servers means that it is interested in discovering servers used to control ICS devices in the network.

In 2017, the first attack to target safety instrumented systems was uncovered in the form of Trisis — so named because it targeted Schneider Electric’s Triconex® Safety Instrumented System (SIS) solutions.³³ While the Trisis campaign was focused on the energy industry in the Middle East, Triconex itself is used in a variety of industries that need constant monitoring and alert for production, equipment, and personnel safety. The Trisis campaign involved several pieces of malware designed to look for and modify the thresholds and logic in Triconex. Unauthorized and malicious alteration of logic can allow a piece of equipment to run too hot or too cold, which in turn can affect performance, reliability, and safety.

These are cases where the security industry has seen traditional malware being used to target systems in the OT environment. In all these cases, the malware families were designed to scan for ICS systems from the IT network, which highlights the importance of securing the IT network in the age of IT and OT network convergence. So far (and quite fortunately), we have not seen malware that is designed to infect and propagate from HMI to HMI or from PLC to PLC, even though researchers have demonstrated in 2015 that this is possible.³⁴

4. IP Threats

Another unique characteristic of the manufacturing industry is the presence of IP in digital form. Digital IP content is extremely important in Industry 4.0. The content can be a product design, a manufacturing process, or information (which can be anything from product recipes and formulas to patented substances and even DNA). IP is a common source of competitive advantage and is thus heavily guarded. For example, the recipe for making the popular Coca-Cola® soft drink is considered one of the most closely guarded trade secrets in the world and is the foundation of the eponymous company's US\$35-billion empire.³⁵

In the manufacturing industry, IP can take the form of a computer-aided design (CAD) file or a document file. CAD files serve as the digital blueprint for physical products, while document files often contain technical specifications, manufacturing processes, recipes, or inspection and quality assurance records. Both of these file types can be infected by viruses or trojanized to aid attackers in gaining access to critical machines.

Poor security configurations can also lead to unintended leakage of proprietary information. Although there is a need for manufacturers to share some information with their suppliers and partners, unsecure defaults risk exposure of information to the public.

4.1 Malicious CAD Files

As indicated in Figure 17, the manufacturing industry has the highest number of detections of malicious CAD files. CAD files can be trojanized by abusing the Visual Basic for Applications (VBA) functionality AutoLISP in the popular AutoCAD® software. While most malicious CAD files belong to the Bursted or Passdoc file-infecting viruses, every once in a while, we see other families targeting CAD files.

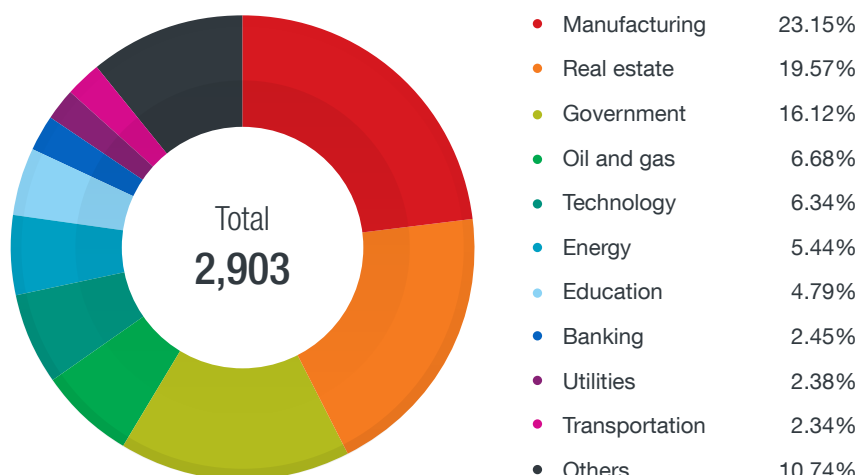


Figure 17. Malicious CAD file detections across industries, based on data from the Trend Micro Smart Protection Network infrastructure for the period from October to December 2018

For instance, the CAD malware family called ACM_SHENZ.A, which was discovered in 2013, is known to weaken the security of infected computers for further attacks.³⁶ The malware creates a user with admin privileges (which can be used later by an attacker to issue commands), creates writable network shares, and opens ports and services that have vulnerabilities.

Malicious CAD files can also be used for industrial espionage. Some attackers have figured out a way to use CAD malware to steal IP and confidential information from infected computers. The CAD malware ACM_MEDRE.AA, for example, looks for PST (personal storage) files in the Microsoft® Outlook® personal information manager as well as CAD files in the infected machine and sends them to a predefined email address.³⁷ By doing so, the attacker receives not only the design and product information contained in the CAD files but also the email communication stored in the PST files of the affected computer.

As for Bursted and Passdoc, they continue to be the top CAD malware families despite dating back to the early 2000s. We looked into the file characteristics of Bursted and Passdoc infections and found that a lot of detections came from external drives (drives E:, F:, etc.), backup software such as FastCopy, or network file sharing services such as Cloud Station. This suggests that a considerable number of the CAD files were infected when they were backed up or archived, and that they lay dormant until someone needed to access them — perhaps for reference in the creation of new or add-on products, design improvement, or consolidation of company IP during a merger or acquisition.

This situation affords insights on the manufacturing industry's security posture years ago, when infected files were backed up or archived. This also shows how old, dormant malware can create internal outbreaks when accessed after being archived for years.

4.2 Microsoft Word Macros

Documents created with the Microsoft® Word® application also have specific uses in the manufacturing industry. But unlike CAD files that contain product designs and information, Word documents in a manufacturing industry setting typically contain manuals and technical information such as parts lists, design specifications, or business-related matters such as order details, terms of service, and warranty information. Similar to the situation of old infected CAD files, some companies have information stored in Word documents that may have been kept in old, isolated machines or archived in data storages for future reference. This creates a situation where infected Word documents lie dormant and undiscovered until accessed or until the machine storing them is connected to the IT network. Decades-old design references, product documentation, recipes, and supplier lists, among others, stored in Word documents could run the risk of being the source of infection in the network. This is worth noting because the Word 97 macro (W97M) is one of the top detections in the manufacturing industry.

In our data, around 10 percent of W97M detections in the manufacturing industry come from Word documents being shared via WeChat, a popular messaging platform in China and Chinese-speaking regions. Unfortunately, document sharing between departments, vendors, and third parties also poses security risks in the form of information leakage and infected documents.

Unauthorized sharing of documents can lead to information leakage. Document sharing is properly done only on corporate-approved channels for auditing and paper trail. This requirement is aimed at maintaining the ability to track with whom a particular IP is shared and whether the sharing is authorized. If documents containing IP are shared through nonstandard channels, then the audit trail is lost and access policies cannot be enforced. A corporate email server, for example, can track which documents are sent or received, which cannot be done on most social media platforms like WeChat. Documents shared on messaging and other social media platforms may also turn out to have been infected with malware, designed to be a phishing lure, or trojanized with exploits.

The issue of old software leading to greater insecurity also plays a role here, as most of the W97M detections are opened using older versions of the Microsoft® Office application suite. Older versions of Office do not have restrictive policies and actions regarding malicious macros, which makes the execution more likely on affected machines. Based on our data, most W97M detections are from machines running Office 2010 or older, which does not have all of the available macro protection features built in.

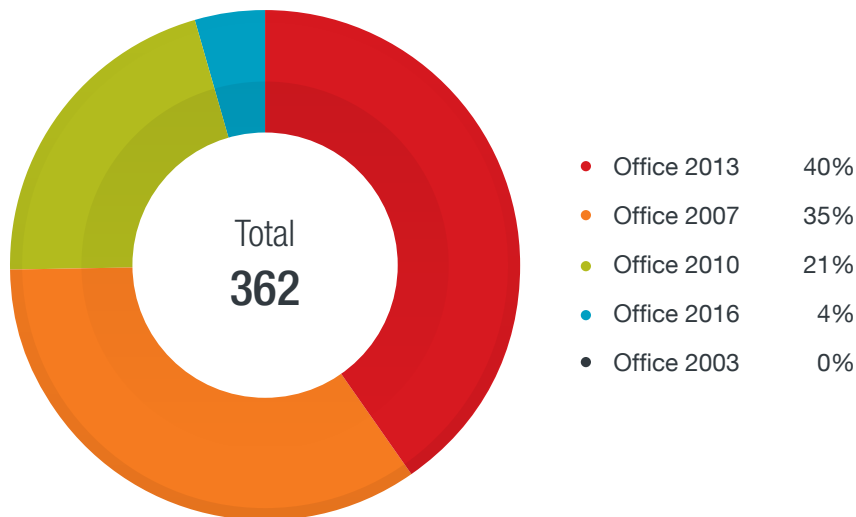


Figure 18. Microsoft Word 97 macro (W97M) detections by Microsoft Office version, based on data from the Trend Micro Smart Protection Network infrastructure for the period from October to December 2018

Version	Support	Default macro behavior	Block from the internet	Trusted locations	Require digital signature	Block per application
Office 2016	Supported until 2025	Block until the user clicks the <i>Enable Macros</i> button	Yes	Yes	Yes	Yes
Office 2013	Supported until 2023	Block until the user clicks the <i>Enable Macros</i> button	Yes*	Yes	Yes	Yes
Office 2010	Supported until 2020	Block until the user clicks the <i>Enable Macros</i> button		Yes	Yes	Yes
Office 2007	Supported until 2017	Block until the user clicks the <i>Enable Macros</i> button			Yes	Yes
Office 2003	Not supported	Macros run automatically			Yes	Yes

*The feature was added to Office 2013 by Microsoft Update.

Table 2. Comparison of versions of Microsoft Office, which includes Microsoft Word, from the National Cyber Security Centre³⁸

Corporate websites of manufacturing companies also need to have proper security configurations in order to prevent data leaks. It is a common practice to share design documents with vendors, suppliers, and third parties through a company's File Transfer Protocol (FTP) server, which is usually also the web server. Poor security configuration can expose these proprietary design documents to the internet and lead to data leakage.

Using simple open-source intelligence (OSINT) techniques, we were able to find CAD files that we believe were not supposed to be exposed to the public.

Index of /CAD/DWG

[Parent Directory](#)

Name	Last modified	Size	Description
10608207-030308.dwg	2012-05-04 12:20	70K	
10608259-081111.dwg	2012-05-04 12:20	74K	
10908207-030308.dwg	2012-05-04 12:20	78K	
10908259-010511.dwg	2012-05-04 12:20	88K	
10908711-080706.dwg	2012-05-04 12:20	561K	
10908711-080706.dwg	2012-05-04 12:20	130K	
2000008092N.dwg	2016-08-02 17:12	254K	
2000008206N-092006.dwg	2012-05-04 12:20	125K	
2000008207N-030308.dwg	2012-05-04 12:20	216K	
2000008217L-112608.dwg	2012-05-04 12:20	264K	

[Index of downloads/CAD](#)

[Parent Directory](#) - [AIR.dwg](#) - [25-Mar-2014 01:10 34K ALEX.dwg](#) - [19-Mar-2014 04:47 370K AIR.dwg](#) - [19-Mar-2014 04:53 12M Arma_Casadeus.dwg](#) - [19-Apr-2011 08:35 10K Angeli_Casadeus.dwg](#) - [07-Jun-2011 03:45 698K Ava_Casadeus.dwg](#) - [07-Jun-2011 03:45 48K BERGEN.dwg](#) - [19-Mar-2014 04:50 59K BRANDO.dwg](#) - [19-Mar-2014 04:50 59K Barcelona_Casadeus.dwg](#) - [19-Apr-2011 08:35 168K Brown_Casadeus.dwg](#) - [19-Apr-2011 08:35 130K Bizarreo_Casadeus.dwg](#)

[Index of](#)

- PLAB20DS DWG 05-Sep-2004 21:53 29K [] PLAB25SL DWG 05-Sep-2004 21:53 29K []
- PLAB25SR DWG 05-Sep-2004 21:53 29K [] PLAB32SR DWG 05-Sep-2004 21:53 61K []
- PLAB32GS DWG 05-Sep-2004 21:53 23K [] PLAB32SL DWG 05-Sep-2004 21:53 29K []
- PLAB32SR DWG 05-Sep-2004 21:53 29K [] PLAB33VA DWG 05-Sep-2004 21:53 53K []
- PLAB40DS DWG 05-Sep-2004 21:53 42K [] PLAB43SL DWG 05-Sep-2004 21:53 33K []
- PLAB40SR DWG 05-Sep-2004 21:53 ...

[Index of](#)

- FINDER.DAT 05-Sep-2004 21:53 1.4K [] PLMB25DS.DXF 05-Sep-2004 21:53 86K [] PLMB25SL.DXF 05-Sep-2004 21:53 91K [] PLMB25SR.DXF 05-Sep-2004 21:53 87K [] PLMB2ZVA.DXF 05-Sep-2004 21:53 188K [] PLMB32SD.DXF 05-Sep-2004 21:53 76K [] PLMB32SL.DXF 05-Sep-2004 21:53 83K [] PLMB32SR.DXF 05-Sep-2004 21:53 83K [] PLMB33VA.DXF 05-Sep-2004 21:53 161K [] PLMB40DS.DXF 05-Sep-2004 21:53 123K [] PLMB40SL.DXF 05-Sep-2004 21:53 99K []

[Index of](#)

[Index of home/dwg](#) - Name - Last modified - Size - Description - Parent Directory - public_html - 2015-10-14 14:35 ..

[Index of](#)

[Parent Directory](#) - [AXLRBHA135.dwg](#) - [AXLRBHA150.dwg](#) - [AXLRBHA165.dwg](#) - [AXLRBHA180.dwg](#) - [AXLRBHA195.dwg](#) - [AXLRBHA210.dwg](#) - [AXLRBHA225.dwg](#) - [AXLRBHA240.dwg](#) - [AXLRBHA255.dwg](#) - [AXLRBHA270.dwg](#) - [AXLRBHA285.dwg](#)

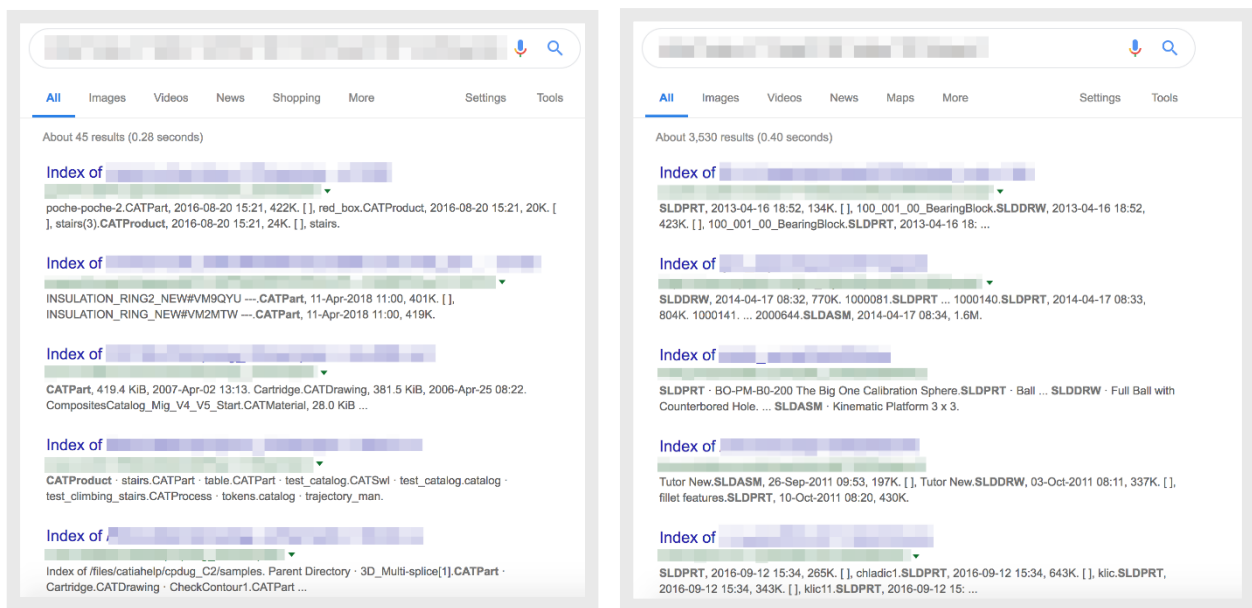


Figure 19. Search results for CAD files via OSINT

5. Underground Activities Related to the Industrial and Manufacturing Sectors

Although industrial cyberespionage has normally been the realm of advanced and persistent attackers, we have seen increasing cybercriminal interest in targeting the industrial and manufacturing sectors.

Figure 20 shows an example of someone posting in a popular underground forum to solicit confidential information, including CAD and computer-aided manufacturing (CAM) files, source code, and confidential documents, for industrial espionage.

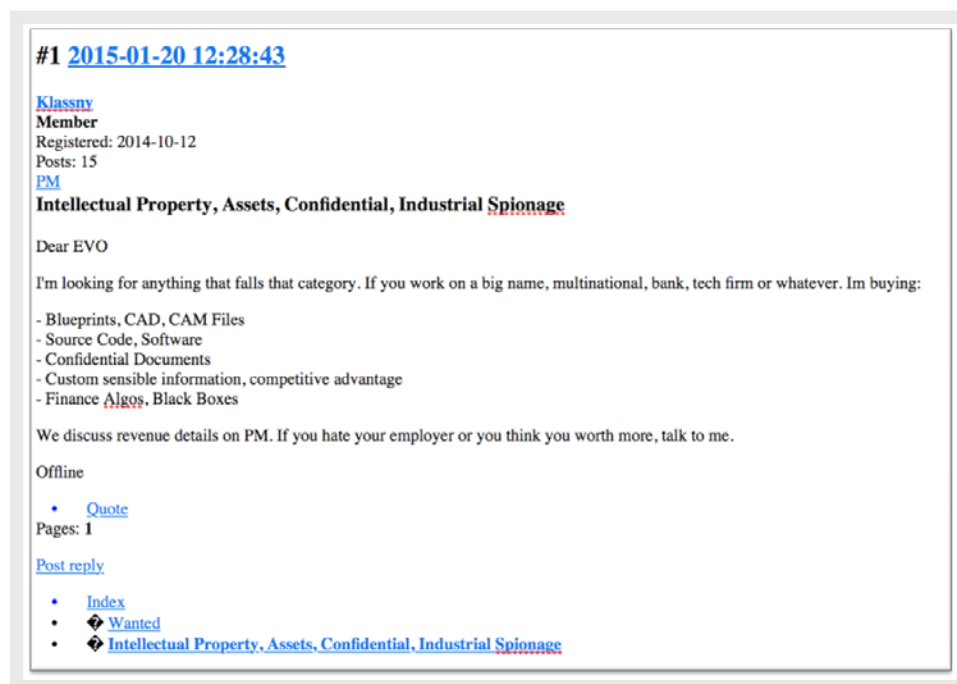


Figure 20. Posting in an underground forum by a user looking for IP assets and other confidential information

We have also been seeing ICS/SCADA-specific hacking tools being sold and advertised online. Figure 21 shows two examples of tools that can be used to crack or brute-force the passwords of PLCs. Although there are OT administrators or engineers who use these tools legitimately, the gray nature of these crackers makes it possible for attackers to read and modify the logic of hacked PLCs. In fact, the National Police Agency of Japan issued in 2015 a notification regarding an observed increase in scanning activity related to PLCs.³⁹

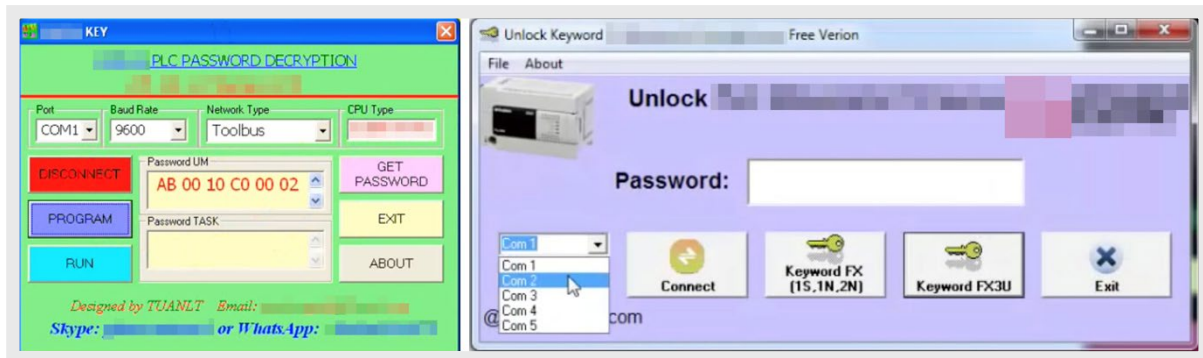


Figure 21. Two examples of PLC password crackers sold online

Taken individually, these activities may seem insignificant. But they are indicative of an increase in cybercriminal interest in tool development and activity targeting the industrial and manufacturing sectors. We predict that in a few years, industrial espionage will not only be performed by persistent attackers, but will also become commoditized with tools and services created and offered by common cybercriminals.

6. Consequences of Security Breaches

We can categorize the impact of cyberthreats to and cyberattacks on the manufacturing industry into two types: production disruption and market disruption.

6.1 Productivity Impact Through Production Disruption

The modern manufacturing industry uses computers to control or monitor the production process in a variety of ways, from operating machines in the manufacturing line to sorting inventories, orders, and shipments of parts and finished products. Indeed, computers play vital roles in the running of a manufacturing facility. Unfortunately, this means that any form of disruptive cyberattack in a manufacturing network, be it ransomware or a denial of service (DoS), will disrupt the production process, even if the attack is not on the production system itself. For instance, incidents affecting enterprise systems such as accounting and order management will disrupt the efficiency of production, given the potential for mix-ups among orders, packages, and materials.

Also, the disruption does not end on the missed production hours of the affected manufacturing plant. Manufacturing companies rely on a network of suppliers for materials and components to create the final product. If one of those suppliers, which are often manufacturing companies themselves, misses a delivery due to missed production time, then the other companies in the supply and manufacturing chain will also be affected. This may result in delayed product releases, which can be crucial, especially during peak shopping seasons or if the goal is to be the first to market.

6.2 Business Impact Through Market Disruption

As previously mentioned, IP is a source of competitive advantage for manufacturing companies. Leaked or stolen IP may not have the immediate impact of a disrupted production line, but the effects are felt long-term.

Leaked design data could be shared not only in the underground but also on legitimate sharing sites. According to a report from March 2018, confidential documents of 186 Japanese companies were shared in a file sharing site in China from June 2017 to February 2018.⁴⁰ Product design files were included in that leak.



Figure 22. Sites showing leaked CAD files pertaining to a popular smartphone

Aside from file sharing sites, stolen design data is also being shared on CAD data sharing sites. While these websites contain generic design information (e.g., the design for an ISO standard screw), some design documents explicitly contain confidential stamps and therefore should not have been shared publicly. Some of these documents may have been stolen through malicious insiders. But cyberespionage and poor cybersecurity practices also contribute to the exposure of proprietary design information.

Probably the greatest impact IP leakage could have is the production of counterfeit products. Counterfeit products are a serious global issue, so much so that the likes of the International Criminal Police Organization (Interpol)⁴¹ and the United Nations Office on Drugs and Crime (UNODC)⁴² are fighting against this crime in the manufacturing industry.

According to the United Nations (UN), counterfeit goods amount to US\$250 billion of trades every year.⁴³ Unfortunately, it seems that there is no end in sight for the situation. In Japan and other advanced industrial nations, counterfeit products are of such high quality that they can easily pass for the originals. These counterfeit goods, known as “supercopy” products, are almost the same as the original products, since the design, materials, and tools used to manufacture them are the same. This hurts the companies that make the original products, as they invest millions of dollars in research, design, and engineering, only to be undercut by counterfeit manufacturers.

7. Security Recommendations

Below are some recommendations that we believe will be most useful for manufacturing companies adopting Industry 4.0.

7.1 Basic Security Principles

Traditional IT systems have long applied basic security principles to secure systems and data. Here are some basic security practices that can address some of the security concerns we have observed to be prevalent in the manufacturing industry.

- **Restrict user access and permissions.** Access should be given only to trusted entities and the most restrictive permission should always be given. For example, the people who are allowed to see confidential or proprietary information should be identified; if they should not be able to modify the data, read-only access should be given to them.
- **Enforce domain or subnetwork restrictions.** The main motivation for converging IT and OT networks is to enable data exchange between control systems and production machines for efficiency and safety. But this does not mean that every laptop or desktop in the IT network should be able to access any of the production machines. It would be ideal to restrict which machines can talk with one another to provide a level of isolation and control on the communications between production machines (which can cost tens, even hundreds, of thousands of dollars).
- **Disable directory listing.** Similar to restricting user access and permissions, ensuring that file and web servers have restricted access to only the people who need to read, modify, or create files is recommended.
- **Remove or disable unnecessary services.** In a semi-isolated environment, not all networking services are used. Identifying and removing or disabling unnecessary services can prevent potential security issues should a vulnerability is exploited on a particular service.

7.2 Asset Identification, Prioritization, and Protection Application

One of the effects of having the OT network connected to the IT network is the introduction of nontraditional devices (e.g., those that are not desktops, laptops, or servers). This puts the IT administrator in an unfamiliar situation and the OT engineer in an IT world, with each role carrying different mindsets and priorities. The IT engineer has the mindset of protecting the data, while the OT engineer prioritizes safety and continuous operation over security. Here are some recommendations to address this situation.

Cooperation

Industry 4.0 brings together CPSs, which means that people addressing the cyber part (IT) should work in harmony with the people working on the physical part (OT). Both teams should agree on how to best support the business by working together to ensure uninterrupted production, keeping IP protected, and doing everything with consideration to safety and efficiency.

Each role brings unique insights to the table. The OT engineer is knowledgeable about the operation of the machines and the input and data needed to make the machines work. The IT engineer is knowledgeable about networking and best security practices. Having shared goals for the OT engineer and IT engineer will force them to work together rather than protect their respective “turfs.”

Accounting and Prioritization of Assets

All assets that get connected to the IT network should be accounted for, including those coming from the OT network. In the context of the industrial internet of things (IIoT), production machinery is treated as IT assets too. The operating systems, necessary software, and services for each should also be mapped out. This will give visibility to the administrators as to which assets to protect. Furthermore, it will be useful as a quick guide during security incidents, network migration, or even standard patch and update cycles as to what services and ports will be affected.

Also, not everything can be protected and security budgets are most likely limited. A paper by a team of researchers from Singapore and the U.K. proposes a discrete mathematical model to calculate for the damage index (DI) and vulnerability index (VI) in order to help highlight which systems in a manufacturing environment need to be secured.⁴⁴ This ensures that all systems in the IT and OT environments are accounted for and are assessed according to how critical they are for the operation and the potential impact each carries should it be compromised or disabled.

Application of Appropriate Protection

As seen on our data, the use of old or unsupported software such as Windows XP is relatively pronounced in manufacturing environments. This correlates with the prevalence of old network-based worms such as Downad in these environments. Since Windows XP is now unsupported (i.e., there will no longer be security patches or updates for it), administrators cannot rely on patching to address security issues that may arise from its continued use.

This situation is also applicable in general to OT systems, as these systems are expected to operate with minimal interruption. This in turn leads to a situation where security patches and software updates are not applied so as to avoid the risk of triggering a failure due to incompatibility, a poor patch, or an update release.

One solution to this challenge is to set up an isolated test environment that replicates the equipment and systems of the production environment. Patch updates and new software versions are then applied to this environment and tested for failures, crashes, or general interference to the operations. If there are no faults, the patch or software updates can be rolled out into the production environment with a degree of confidence that they would work and that they would not cause any unintended consequences when deployed.

The downside to the aforementioned solution is that it could be expensive to implement. An alternative is to use technologies such as virtual patching, intrusion detection systems (IDSs), and application control, which provide sufficient protection without the heavy footprint and with less risk of interfering with machine operations.

7.3 User Education

Also reflected in our data is the common practice of sharing documents using messaging and other social media platforms. While there are technologies that can be used to address this by restricting software installed in computers, it would be better to educate personnel about the value of documents containing IP and other proprietary information and the need to protect them.

7.4 Making Security a Requirement

As manufacturing facilities introduce Industry 4.0 technologies to their existing or new facilities, decision makers need to make security a requirement during the procurement process. As previously mentioned, manufacturing equipment has a life span of up to about 35 years. Thus, cybersecurity features need to be integrated into the design of the equipment in order to make maintenance and protection easier in a highly connected factory network. Otherwise, the cybersecurity team will be forced to implement less than optimal workaround solutions that may cost more to implement or be difficult to set up and maintain.

Making security a requirement sends a message to the vendors that security is a clear need, and may urge them to design products that are more secure and enabled in Industry 4.0 environments.

7.5 IEC 62443 Compliance

Another recommended approach to securing manufacturing companies adopting Industry 4.0 is to align with the IEC 62443 cybersecurity standards,⁴⁵ which include the aforementioned recommendations. They cover several aspects such as requirements for an ICS security management system, security technologies for ICSs, and secure product development life cycles. They are widely referred to as industrial standards for asset owners, system integrators, and device manufacturers.

8. Conclusion

The manufacturing industry's adoption of Industry 4.0, as exemplified by the implementation of connected production and the setting up of smart factories, presents a drastically different cyberthreat risk profile from that which arose out of the adoption of Industry 3.0. While Industry 4.0 maps out the ideal state for helping manufacturing companies and economies remain competitive, there is so far no specification or guideline for secure practices and implementation. Unlike the financial industry, manufacturing does not have the benefit of having clear standards and regulations laid out in regard to handling, processing, and securing the interconnection of systems, processes, and data.

The convergence of IT and OT networks introduces device classes into the IT network that are either outdated or possibly vulnerable. This calls for IT administrators to work with process engineers and equipment operators in order to accomplish certain tasks: auditing new equipment, identifying the underlying operating systems and platforms, and figuring out the required ports, protocols, routing, and services to adequately secure IIoT systems as they are connected to the IT network.

IP in the form of documents and design files introduces unique types of malware threats, as these two formats have macro and scripting capabilities that are being abused by malicious actors.

Lastly, the consequences of a successful security breach in an Industry 4.0 environment goes far beyond the immediate cost of outbreak containment and the corresponding cleanup. Destructive attacks such as those involving ransomware can halt the production line and incur significant monetary losses. The impact of stolen or leaked IP, meanwhile, can affect sales and market share through the proliferation of supercopy products.

While Industry 4.0 enables efficiencies and economic advantages, adopters need to be aware of the new cyberthreat risk profile associated with it. They need to consider the security implications, design networks, technologies, processes, and reporting lines that will address the new environments being ushered in.

References

1. Sophia Yan. (27 February 2017). *CNBC LLC*. “‘Made in China’ isn’t so cheap anymore, and that could spell headache for Beijing.” Last accessed on 15 March 2019 at <https://www.cnbc.com/2017/02/27/chinese-wages-rise-made-in-china-isnt-so-cheap-anymore.html>.
2. Shannon Tiezzi. (13 March 2015). *The Diplomat*. “China’s Plan to Dominate World Markets.” Last accessed on 15 March 2019 at <https://thediplomat.com/2015/03/chinas-plan-to-dominate-world-markets/>.
3. Germany Trade & Invest. (n.d.). *Germany Trade & Invest*. “Industrie 4.0.” Last accessed on 15 March 2019 at <https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Industrie-4-0/industrie-4-0-what-is-it.html>.
4. Ministry of Electronics & Information Technology Government of India. (13 March 2019). *Digital India*. “About Digital India.” Last accessed on 15 March 2019 at <https://digitalindia.gov.in/content/about-programme>.
5. Ministry of Economy, Trade and Industry. (1 February 2019). *Ministry of Economy, Trade and Industry*. “Connected Industries.” Last accessed on 15 March 2019 at https://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html.
6. Ksenia Lukian. (23 July 2017). *Vesti.ru*. “4.0.RU: новая модель промышленного производства.” Last accessed on 15 March 2019 at <https://www.vesti.ru/doc.html?id=2912970>.
7. Industrial Internet Consortium. (n.d.). *Industrial Internet Consortium*. “ABOUT US.” Last accessed on 15 March 2019 at <https://www.iiconsortium.org/about-us.htm>.
8. Trend Micro. (n.d.). *Trend Micro*. “Internet of Things (IoT).” Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/security/definition/internet-of-things>.
9. Trend Micro. (8 August 2018). *Trend Micro Security News*. “A Look Into Smart Factories: A Model of IIoT Innovation.” Last accessed on 21 March 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/a-look-into-smart-factories-a-model-of-iiot-innovation>.
10. Bundesministerium für Bildung und Forschung. (n.d.). *Bundesministerium für Bildung und Forschung*. “Industrie 4.0.” Last accessed on 21 March 2019 at <https://www.bmbf.de/de/zukunftprojekt-industrie-4-0-848.html>.
11. Trend Micro. (n.d.). *Trend Micro*. “Industrial Internet of Things (IIoT).” Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot>.
12. Abdul Azeez Erumban. (2 June 2008). *The Review of Income and Wealth*. “Lifetimes of Machinery and Equipment: Evidence from Dutch Manufacturing.” Last accessed on 15 March 2019 at <http://www.roiw.org/2008/2008-11.pdf>.
13. Trend Micro. (7 December 2017). *Trend Micro*. “CONFICKER/ DOWNAD 9 Years After: Examining its Impact on Legacy Systems.” Last accessed on 15 March 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/conficker-downad-9-years-examining-impact-legacy-systems/>.
14. Microsoft Lifecycle Policy. (n.d.). *Microsoft*. “Search product lifecycle.” Last accessed on 20 March 2019 at <https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%20XP>.
15. Trend Micro. (13 May 2017). *Trend Micro*. “WannaCry/Wcry Ransomware: How to Defend against It.” Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/wannacry-wcry-ransomware-how-to-defend-against-it>.

16. Jessa De La Torre. (29 October 2012). *Trend Micro*. "Gamarue Malware Goes to Germany." Last accessed on 15 March 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/gamarue-malware-goes-to-germany/>.
17. Danielle Veluz. (1 October 2010). *Trend Micro*. "STUXNET Malware Targets SCADA Systems." Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems>.
18. Ryan Angelo Certeza. (4 October 2012). *Trend Micro*. "Pulling the Plug on PlugX." Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx>.
19. The MITRE Corporation. (n.d.). *MITRE ATT&CK*. "DLL Search Order Hijacking." Last accessed on 15 March 2019 at <https://attack.mitre.org/techniques/T1038/>.
20. Alvin Bacani. (30 June 2017). *Trend Micro*. "HKTL_MIMIKATZ." Last accessed on 15 March 2019 at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/hktl_mimikatz.
21. Tencent. (17 April 2018). *Tencent*. "黑客入侵加密企业所有服务器 嚣张留言勒索9.5比特币." Last accessed on 15 March 2019 at <https://s.tencent.com/research/report/461.html>.
22. CoinMarketCap. (n.d.). *CoinMarketCap*. "Bitcoin." Last accessed on 20 March 2019 at <https://coinmarketcap.com/currencies/bitcoin/>.
23. Jon Sharman. (13 May 2017). *Independent*. "Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France." Last accessed on 20 March 2019 at <https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html>.
24. Yimou Lee. (6 August 2018). *Reuters*. "Apple chip supplier TSMC resumes production after WannaCry attack." Last accessed on 15 March 2019 at <https://in.reuters.com/article/taiwan-tsmc-virus/apple-chip-supplier-tsmc-resumes-production-after-wannacry-attack-idINKBN1KR0B9>.
25. Trend Micro. (20 March 2019). *Trend Micro Security News*. "What You Need to Know About the LockerGoga Ransomware." Last accessed on 26 March 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware>.
26. John Leyden. (6 August 2018). *The Register*. "Chip flinger TSMC warns 'WannaCry' outbreak will sting biz for \$250m." Last accessed on 15 March 2019 at https://www.theregister.co.uk/2018/08/06/tsmc_malware/.
27. Emery Dalesio. (9 August 2017). *Citizen Times*. "Hackers looking to shut down NC factories for pay." Last accessed on 15 March 2019 at <https://www.citizen-times.com/story/money/business/2017/08/09/hackers-looking-shut-down-nc-factories-pay/104431058/>.
28. Yacin Nadji et al. (2011). *Astrolavos Lab*. "Understanding the Prevalence and Use of Alternative Plans in Malware with Network Games." Last accessed on 15 March 2019 at <https://astrolavos.gatech.edu/articles/gzaacsac2011.pdf>.
29. Trend Micro Zero Day Initiative Team. (23 May 2017). *Trend Micro*. "The State of SCADA HMI Vulnerabilities." Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities>.
30. Stephen Hilt et al. (30 October 2018). *Trend Micro*. "Critical Infrastructures Exposed and at Risk: Energy and Water Industries." Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries>.
31. Kyle Wilhoit and Jim Gogolinski. (16 October 2014). *Trend Micro*. "Sandworm to Blacken: The SCADA Connection." Last accessed on 15 March 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/>.

32. Kyle Wilhoit. (17 July 2014). *FireEye*. "Havex, It's Down With OPC." Last accessed on 15 March 2019 at <https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html>.
33. Trend Micro. (22 December 2017). *Trend Micro*. "TRITON Wielding its Trident – New Malware tampering with Industrial Safety Systems." Last accessed on 15 March 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems>.
34. Ralf Spenneberg, Maik Bruggemann, and Hendrik Schwartke. (2016). *Black Hat*. "PLC-Blaster: A Worm Living Solely in the PLC." Last accessed on 15 March 2019 at <https://www.blackhat.com/docs/us-16/materials/us-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf>.
35. The Coca-Cola Company. (23 February 2018). *United States Securities and Exchange Commission*. "Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 For the fiscal year ended December 31, 2017." Last accessed on 20 March 2019 at http://d18rn0p25nwr6d.cloudfront.net/CIK-0000021344/f2a7de17-c60e-49c2-97ee-9abfad26eb85.pdf#A2017123110-K_HTM_SC9692856C7A05677AA0B95DDD6369B06.
36. Anthony Joe Melgarejo. (22 November 2013). *Trend Micro*. "AutoCAD Malware Leaves Victims Hackable." Last accessed on 15 March 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/autocad-malware-leaves-victims-hackable/>.
37. Christopher Daniel So. (28 June 2012). *Trend Micro*. "ACM_MEDRE.AA." Last accessed on 15 March 2019 at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/acm_medre.aa.
38. National Cyber Security Centre. (21 February 2019). *National Cyber Security Centre*. "Macro Security for Microsoft Office." Last accessed on 15 March 2019 at <https://www.ncsc.gov.uk/guidance/macro-security-for-microsoft-office>.
39. National Police Agency. (5 June 2015). *National Police Agency*. "産業制御システムで使用する PLC の脆弱性を標的としたアセスの観測について (第2報)." Last accessed on 15 March 2019 at <https://www.npa.go.jp/cyberpolice/detect/pdf/20150605.pdf>.
40. Nikkei. (1 March 2018). *Nikkei Inc.* "止まらぬ日本企業の文書流出 中国サイトに186社分." Last accessed on 15 March 2018 at <https://www.nikkei.com/article/DGXMZO2756453001032018CR8000/>.
41. International Criminal Police Organization. (n.d.). *INTERPOL*. "Illicit Goods and Global Health." Last accessed on 15 March 2019 at https://www.interpol.int/es/content/download/5263/file/Illicit_goods_and_global_health.pdf?inLanguage=eng-GB.
42. United Nations Office on Drugs and Crime. (n.d.). *UNODC*. "COUNTERFEIT Don't Buy Into Organized Crime." Last accessed on 15 March 2019 at <https://www.unodc.org/counterfeit/>.
43. United Nations. (14 January 2014). *United Nations*. "New UN campaign spotlights links between organized crime and counterfeit goods." Last accessed on 15 March 2019 at <https://news.un.org/en/story/2014/01/459622-new-un-campaign-spotlights-links-between-organized-crime-and-counterfeit-goods>.
44. Vinayak Prabhu et al. (25 July 2018). *SpringerLink*. "Towards Data-Driven Cyber Attack Damage and Vulnerability Estimation for Manufacturing Enterprises." Last accessed on 27 March 2019 at https://link.springer.com/chapter/10.1007%2F978-3-319-95678-7_38.
45. SA Security Compliance Institute. (n.d.). *ISA Secure*. "Securing Control Systems using IEC 62443 Standards." Last accessed on 20 March 2019 at https://www.isasecure.org/en-US/Documents/Articles-and-Technical-Papers/2018-IEC-62443-and-ISASecure-Overview_Suppliers-Pe.



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 threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com



| research 