

Honeywell

THE POWER OF **CONNECTED**

Honeywell Industrial USB Threat Report

Universal Serial Bus (USB) threat vector trends and implications for industrial operators





OVERVIEW

These are interesting times for Universal Serial Bus (USB) security. With increasing pressure to limit network access to industrial control systems, industrial plant dependence upon USB removable media to transfer information, files, patches and updates has been greater than ever. At the same time, past research into USB threats has shown that portable USB drives are one of the top threat vectors impacting industrial control systems (Source: BSI, 2016).

While this is notable enough on its own, USB represents an even greater threat than spreading malware: a USB device can be used to attack systems directly, using the USB interface as a powerful attack vector. Malicious USB devices crafted specifically to attack computers via the USB interface have become readily available for purchase online, while BadUSB – a technique that turns USB devices such as fans and charging cables into potential attack vectors – has increasingly been weaponized.

In context of these USB security concerns and ongoing threat vector changes, researchers from Honeywell's Industrial Cyber Security team analyzed USB usage and behavioral data from live production sites globally. This report shares findings from these research activities and presents USB threat trends. Discussion of potential impact to operational facilities is also discussed. A [glossary](#) of terms used in this report is offered at the end of this document.

This report shares Honeywell USB security research findings to advance industry dialogue and threat prevention collaboration, in hopes of lowering cyber attack risk to industrial operations worldwide.


Methodology

USB usage and behavioral data was extracted from a proprietary, globally deployed Honeywell security platform, Secure Media Exchange (SMX). Since SMX analyzes USB devices used in industrial facilities, it provides a highly relevant snapshot into industrial USB activity.

Data collected from SMX is anonymous with no personally identifiable information (PII), and only a sample set of all SMX data was analyzed. As such, findings represent consolidated views into the collective data set, and sample set findings are interpreted in light of impact upon the larger sample set.

Industries represented include Oil & Gas, Energy, Chemical Manufacturing, Pulp & Paper, and other industrial manufacturing facilities. No detailed correlation to region, nor detail by industry, has been provided here, in an effort to further preserve data anonymity.

The sample set consisted of 50 locations where SMX is deployed in live production environments. Data was collected from across the US, South America, Europe, and the Middle East. This sample set represents files actively carried into production control facilities via USB removable storage devices, during normal day-to-day operations.



50
Locations



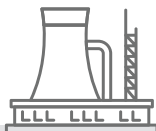
4
Continents



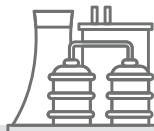
4+
Industries



Oil & Gas



Energy



Chemical



Pulp & Paper

KEY FINDINGS

USB Remains a Top Threat Vector

Of the locations studied, nearly half (44%) detected and blocked at least one malicious or suspicious file that represented a security issue. This high-level finding confirms that USB remains a significant vector specifically for industrial threats. The data also indicates that risk of industrial facility exposure to threats via USB is consistent and statistically relevant. This data finding is consistent with other third party reports that cite USB as a major threat vector.



44%
of SMX Locations
Detected & Blocked
at Least One
Suspicious File

USB-Borne Malware: A High-Potency Threat

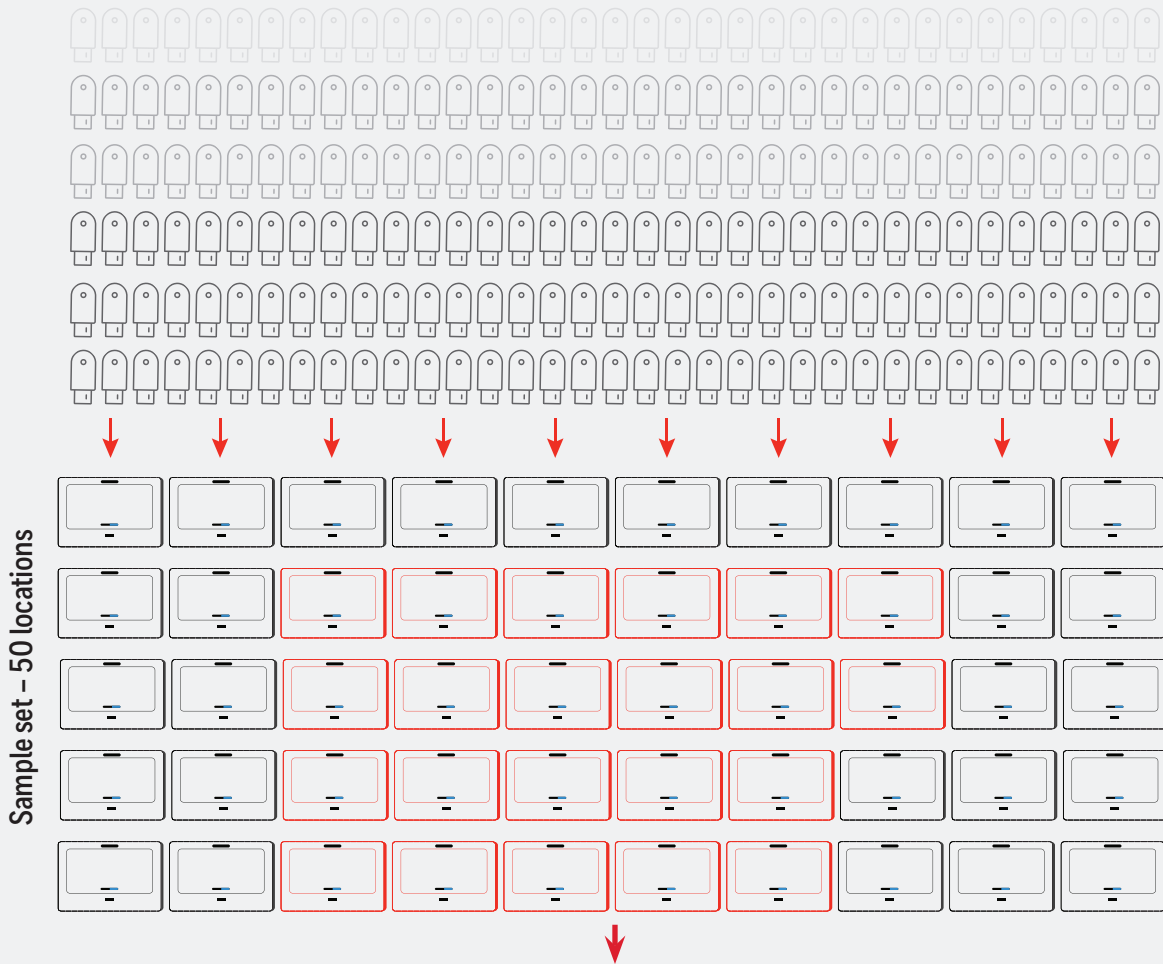
While the volume of malware discovered in this research was small relative to the total sample size volume, the malware potency was significant. Of those threats blocked by SMX, 1 in 4 (26%) had the potential to cause a major disruption to an industrial control environment, including loss of view or loss of control, and 16% were targeted specifically against Industrial Control System (ICS) or Internet of Things (IoT) systems.



A notable 15% of the total threats detected and blocked were high-profile, well-known threats, including **Stuxnet** (2%), **Mirai** (6%), **TRITON** (2%), and **WannaCry** (1%). It's not the presence of these threats that is concerning; on the contrary, these and other threats have been in the wild for some time. Rather, it's that these threats were attempting to enter industrial control facilities via removable storage devices, in a relatively high density, that is significant.

These findings are worrisome for several reasons. That high-potency threats were at all prevalent on USB drives bound for industrial control facility use is the first concern. As ICS security experts are well aware, it only takes one instance of malware bypassing security defenses to rapidly execute a successful, widespread attack. Second, the findings also confirm that such threats do exist in the wild, as the high-potency malware was detected among day-to-day routine traffic, not pure research labs or test environments. Finally, as historical trends have shown, newly emerging threat techniques such as TRITON, which target Safety Instrumented Systems, can provoke copycat attackers. Although more difficult and sophisticated to accomplish, such newer threat approaches can indicate the beginnings of a new wave of derivative or copycat attacks.

Types of Industrial USB Threats



Of the threats blocked:

26%

Potential to cause major disruption to ICS
e.g. loss of view or loss of control

16%

Targeted ICS or IOT

15%

Are well-known threats
e.g. Mirai, Stuxnet, TRITON, WannaCry

9%

Designed to exploit USB

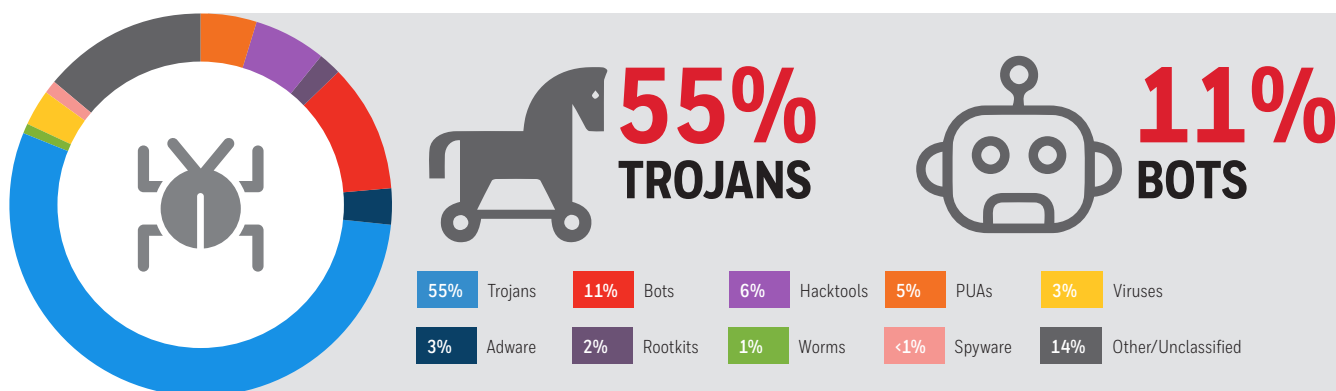
Accidental Infections or Targeted Attacks?

Of the total files known to be malicious, the type and behavior of the malware varied considerably. The most pervasive malware category by far was Trojans, representing 55% of all malware detected. This makes sense in the context of USB-borne malware, where Trojans can be very effective.

Other malware types discovered through this research included bots (11%), hacktools (6%) and Potentially Unwanted Applications (5%).

Of the malware discovered, 9% was designed to directly exploit USB protocol or interface weaknesses, making USB delivery even more effective – especially on older or poorly configured computers that are more susceptible to USB exploits. Some went further, attacking the USB interface itself. 2% were associated with common Human Interface Device (HID) attacks, which trick the USB host controller into thinking there is a keyboard attached, allowing the malware to type commands and manipulate applications. This supports earlier Honeywell findings that confirmed HID attacks such as BadUSB as realistic threats to industrial operators.

Looking at the specific malware families found, a small-but-significant degree of deliberate, targeted behavior was discovered, including such prominent industrial threats as Stuxnet, TRITON and others. As also mentioned earlier, **26% of the threats discovered had the potential to impact industrial control environments, and 16% were specifically targeted against the same environments.**



A Diversity of Malware Functionality, Led by RATs and Droppers

The malware discovered was analyzed to reveal many diverse functionality types, from adware to ransomware. Interestingly, Remote Access Toolkits (RATs) were the most notable functionality used (32%), as well as Droppers (12%) designed to download and install additional malware. This is interesting because best practices dictate that industrial control environments should tightly control outbound connectivity from the industrial control site to the Internet. Proper process control network architecture would prevent all such unauthorized connectivity, making most RATs and Droppers useless. This implies attackers have a reliance upon and expectation of poor network design in the majority of the threats analyzed.

15% were classified as “attacks”, designed to exploit a specific system or application, damage files or end stations, or perform other actions designed to cause immediate harm. While Petya and WannaCry were detected, occurrences were relatively less common (1% each). However, a notable 7% of all threats detected and blocked by SMX were ransomware.

Also discovered through the analysis was an abundance of Potentially Unwanted Applications (PUAs), worms and viruses that were of medium or low severity. Interestingly, these included a relatively high proportion of password cracking tools, illicit browsers, installers, game crackers,

registry editors and other software tools that, while not malicious themselves, are capable of being used maliciously. The relative prevalence of these types of tools is notable considering that, especially in critical industries, these unwanted applications are often prohibited by policy.

While difficult to associate any specific malicious file to a broader campaign, our best efforts indicated that over 50% of the malicious files analyzed had the capabilities of persistence typical of an Advanced Persistent Threat (APT). The prevalence of evasion and enumeration techniques, combined with remote access and installation of additional packages suggest that many of the threats found were intended to gain a remote foothold.

The evidence of a relatively high percentage of threats that targeted ICS, that were capable of impacting ICS, and that exhibited persistence, validates current best practices of deploying strong network defenses and perimeters around critical areas. In this study, such attempts were blocked; however, any organization that allowed such threats to enter the process control network, and allowed outbound network connectivity, would face dangerous consequences from these threats. The findings also illustrate how an attacker, faced with an obstacle, will attempt to find another path – in this case, the use of USB removable storage as an alternate attack vector to direct network attacks.



%		%	
32	Remote Access Toolkits (RATs)	2	USB Attack (HID)
12	Droppers	2	Scanners
10	DDoS	2	Reconnaissance & enumeration tools
8	Attacks	1	Crackers
7	Ransomware	<1	Keyloggers
6	Data theft & exfiltration tools	<1	Flooders
5	Generic	8	Other/Unclassified
4	Crypto-currency miners		

USBs Carry Old and New Threats into the Plant

Both old malware and new threat types were detected in the sample size data. For example, the Conficker worm was detected and blocked. Conficker was first discovered over 10 years ago and is capable of causing serious disruptions to networks. It can limit recoverability by impairing backup services and deleting restore points. Its presence indicates the need to continue checking for known malware of any age, rather than assuming the organization has learned from past incidents.

The presence of the Conficker worm on USB storage media itself is unsurprising, as Conficker uses USB autorun trojans as one method of infection and propagation. It does, however, provide further evidence that such threats exist in day-to-day control system USB usage, outside of intentional malware testing facilities.

As noted in previous sections, relatively new threats such as TRITON were also identified and blocked. While data was inconclusive, researchers estimate that approximately 10% of malware variants were less than one week old.



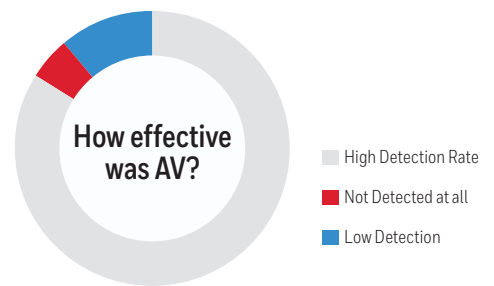
Catching Missed Malware

To determine the efficacy of SMX, the threats uncovered by this study were also analyzed using other commercial security tools. Despite the fact that many threats have been known for some time, 5% of the total threats discovered by SMX were completely undetectable by all commercial anti-malware solutions tested (and remain undetectable at the time this report was written). Further, 11% of the malware variants were only detected erratically and only by a few anti-virus engines. In addition, the estimation that 10% of malware variants were less than a week old at the time of detection is of concern within industrial facilities, where many organizations update anti-virus signatures less frequently. For facilities relying on anti-virus solutions that are out of date, such newer malware variants are completely undetectable.

SMX improves detection performance using a variety of advanced threat detection and threat intelligence technologies, and performs continuous efficacy tests to ensure that SMX is using the best techniques available. While these report findings indicate that SMX is performing well, the severity of the threats discovered warrants the use of additional security measures for true defense-in-depth.



UP TO 11%
of threats discovered by SMX from
the study's sample size were
UNDETECTABLE BY TRADITIONAL AV



Security Implications for Operators

These report findings clearly illustrate the importance of adopting and adhering to common industrial cyber security best practices:

- USB security must include technical controls and enforcement. Relying on policy updates or people training alone will not suffice for scalable threat prevention. Despite the widespread belief that USB drives are dangerous, and despite the prevalence of corporate USB usage policies, the data provides ample evidence that USB hygiene is generally poor.
- Outbound network connectivity from process control networks should be tightly controlled, and such restrictions should be enforced by network switches, routers and firewalls. While USB drives are useful vectors of initial infection, the attack types here reveal a tendency for hackers to establish remote access, and to download additional payloads as needed.
- Security upkeep is important: Anti-virus software deployed in process control facilities needs to be updated daily to be at all effective. Even then, additional protection is recommended, based on the poor detection rates of common AV products when analyzing the threats here.
- Patching and hardening of end nodes is necessary, despite the challenges of patching production systems. While sophisticated and targeted attacks were detected, many old threats were identified and could be easily mitigated by simply keeping the infrastructure current.
- USB security hygiene is poor. Additional cyber security education is required for proper handling and use of removable storage. This is supported by the presence of video game cheat engines, password crackers, and known hack tools found among the samples analyzed. This can and should be addressed through employee and partner awareness programs, operational personnel cyber security training, and sound security policy development.
- Ransomware is a serious threat to industrial facilities. The financial losses of ransomware are easily thwarted by maintaining regular backups and having a tested recovery process in place. It is never ideal to pay a ransom if infected: it is not guaranteed that systems will be restored, and it will encourage further ransomware campaigns to target industrial systems if they are seen as a viable market. For further advice, as well as many ransomware identification and decryption tools, visit <https://www.nomoreransom.org>



Conclusion: Is the Sky Falling?

While the types of threats discovered on inbound USB removable storage were more serious than the research team anticipated, the overall amount of malware was relatively small. The most important findings point to the inevitability of USB threat exposure, with nearly half of the SMX gateways analyzed blocking at least one malicious file. When so many of the threats discovered are targeting ICS and potentially disruptive, every threat needs to be prevented. This report shares Honeywell USB security research findings to advance industry dialogue and threat prevention collaboration, in hopes of lowering cyber attack risk to industrial operations worldwide.



Glossary:

Adware

Adware is malware that is designed to display unwanted advertising material, often in banners or pop-ups. Adware is often considered a nuisance, although the interruptions caused by adware can become serious, especially if the infection is on a critical system, by making it difficult to interact with the computer in a normal manner.

APTs / Advanced Persistent Threats

Advanced Persistent Threat (APT) refers to a class of cyber threat designed to infiltrate a network, remain persistent through evasion and propagation techniques. APTs are typically used to establish and maintain an external command and control channel through which the attacker can continuously exfiltrate data.

Attacks

Malware classified as "Attacks" as opposed to threats refer to malicious programs that attempt to cause real harm by damaging, modifying or destroying data, computer systems, or networks.

Backdoors

Backdoors provide unauthorized access to computer files, systems, or networks. Backdoors that provide access over a network are often referred to as Remote Access Toolkits or RATs, although backdoors may also be specific to local systems or applications.

BadUSB

An exploitation of certain USB devices allowing the firmware to be overwritten by a hacker, to modify how that device operates. Typically used to alter commercially available USB devices, so that they can be used as a cyber attack tool.

Bots

Bots are malicious programs that act autonomously. When bots are distributed across a network (referred to as a botnet), they are capable of carrying out distributed, coordinated actions such as Distributed Denial of Service (DDoS) attacks.

Crackers

Applications designed to bypass passwords or application security measures, either as benign password recovery tools, penetration testing tools, or as attempts to bypass software licensing.

Data Theft & Exfiltration Tools

Data theft & exfiltration tools are malicious programs designed to obtain information from a target computer or network, with the intent of communicating that information back to an attacker located outside of the target network.

DDoS / Distributed Denial of Service

A Denial of Service attempts to disrupt a computer or network to make it unusable. A distributed DoS typically connects to a target simultaneously from many individual computers, flooding it with data and making it unreachable. Distributed attacks generally use a network of bots ("botnets") to coordinate the distributed attack.

Droppers

A Dropper is a malicious program designed to download and install other malicious programs. Droppers typically don't cause harm directly but are designed to 'drop' one or more malware payloads onto a target machine.

Enumerators

Enumeration is the process of identifying valid identities of devices and users in a network; typically as an initial step in a network attack process. Enumerators are applications that attempt to identify valid systems and/or accounts that can then be targeted for exploitation or compromise.

Flooders

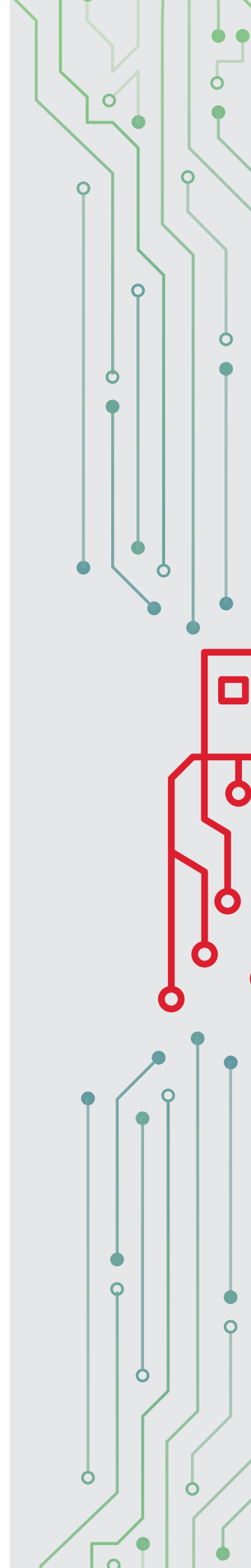
Flooders are malicious programs designed to flood a network, typically to consume bandwidth as part of a Denial of Service attack.

Hacktools

Hacktools are applications used by penetration testers and hackers to perform tasks typically associated with hacking.

Mirai

Mirai is malware designed to infect networked Linux devices, turning them into remotely controlled "bots" that can then be used as part of a botnet in large-scale network attacks. Mirai is notable because it targeted IP cameras and home routers, in what is largely recognized as the first large-scale IoT botnet. Mirai was able to create a DDoS botnet of sufficient size and capacity to take down the "Krebs on Security" website, GitHub, Twitter, Reddit, Netflix and others, as well as several Internet Domain name Servers that took several ISPs offline.





Petya

Petya is a family of ransomware that infects the master boot record, preventing Windows from booting, and also the Master File Table (MFT), making the computer's file system unreadable and extremely difficult to recover. The encryption of the MFT earned Petya notoriety for being the "next step" in the evolution of ransomware. A later variant of Petya, NotPetya, is known for widespread damage to targets, including the Ukraine energy sector. Unlike Petya, NotPetya is self-replicating and easily spread without human interaction. NotPetya is named because, while derived from Petya, it is not ransomware: while it encrypts systems like Petya, it does so to cause damage with no intention of recoverability.

PUAs/Potentially Unwanted Applications

PUAs are applications that are not typically designed to be malicious, but that perform functions that may contradict the security interests of users or that may operate in a manner that could present a cyber security risk.

Ransomware

A type of malware designed to block users from accessing or using a computer system until a ransom is paid. Most ransomware functions by encrypting specific files, the master boot sector, and/or the master file table of a computer. When the ransom is paid, the decryption keys may be provided to allow the restoration of the infected computer. For advice on prevention and remediation of ransomware visit

<https://www.nomoreransom.org>

Secure Media Exchange

Secure Media Exchange Secure Media Exchange (SMX) is a commercial industrial cyber security technical solution developed by Honeywell to lower the risk of USB-borne threats. For more information, visit <https://www.hwl.co/SMX>

Stuxnet

An advanced cyber attack against an industrial control system, consisting of multiple zero-day exploits used for the delivery of malware that then targeted and infected specific industrial controls for the purposes of sabotaging an automated process. Stuxnet is widely regarded as the first cyber attack to specifically target an industrial control system. Stuxnet is also significant in its complexity, as it represented a massive advancement in capability over any previously known malware at the time.

TRITON

TRITON is an industrial control system attack framework capable of writing new application memory to susceptible Safety Instrumented System (SIS) controllers. TRITON allows an attacker to modify SIS behavior under certain conditions. TRITON is considered a critical threat because SIS systems are responsible for independently monitoring an industrial process and initiating a safe shutdown in advance of a hazardous state. TRITON could be used to trigger a shutdown, taking an industrial process offline, or it could potentially be used to prevent a shutdown even when a hazardous state has been reached. In coordination with other ICS attacks, TRITON could increase the chances of causing physical damage via a cyber attack.

Trojan

A Trojan is malware that masquerades as a legitimate application, in order to trick a user into executing it. The term is derived from the Trojan Horse, which tricked the defenders of Troy into carrying hidden Greek troops within the city walls. Unlike computer viruses and worms, Trojans generally do not operate autonomously, instead relying on a user for execution.

USB/Universal Serial Bus

The USB protocol defines how many device types can interconnect to a single computer interface, designed to replace many custom computer peripherals with a single, common interface. The term "USB" could refer to any specific USB device, such as a mouse, keyboard, removable storage, network adapter, et. al.; a USB host, such as a computer or other digital system with a USB interface; or the USB protocol itself.

Viruses

A computer virus refers to malicious software that is capable of "infecting" other computer programs by inserting its own code to modify them.

WannaCry

A ransomware campaign that leveraged the EternalBlue exploit, a nation-state level Windows exploit that was stolen and leaked by a group known as the Shadow Brokers. WannaCry is significant in the scale of its initial infection, which encrypted more than 200,000 computers across 150 countries. Because WannaCry is able to spread and infect other computers across the Internet as well as laterally across a local network, it is classified as a worm.

Worms

A computer worm is a standalone malware computer program that is able to self-replicate by spreading to and infecting other computers.



About Honeywell Industrial Cyber Security

Honeywell is the leading provider of cyber security solutions that protect industrial assets, operations and people from digital-age threats.

With more than 15 years of industrial cyber security expertise and more than 50 years of industrial domain expertise, Honeywell combines proven cyber security technology and industrial know-how to maximize productivity, reliability and safety. We provide innovative cyber security software, services and solutions to protect assets, operations and people at industrial and critical infrastructure facilities around the world. Our state-of-the-art Cyber Security Centers of Excellence allow customers to safely simulate, validate and accelerate their industrial cyber security initiatives.

For more information

To learn more about Honeywell's Industrial Cyber Security Solutions, visit www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Zunyi Road
Shanghai, China 200051

www.honeywellprocess.com