HONEYWELL INDUSTRIAL CYBERSECURITY USB THREAT REPORT 2020

TABLE OF CONTENTS

OVERVIEW

Since publication of our original USB threat report, there has been a general increase in awareness around the potential cyber risk of our friend the Universal Serial Bus. For critical infrastructure operators in manufacturing, aerospace, energy, shipping, chemical, oil and gas, pulp and paper, water and wastewater, and building automation, removable media remains one of the top vectors for cybersecurity threats.

Traditionally, this was because process control and critical networks are typically well-isolated, with strong physical and logical access controls in place; as such, attacks relying on network penetration and intrusion can be more difficult. The remaining "low hanging fruit" for attackers is the need for file transfers into and among industrial automation and control systems. Whether downloading patches from a "trusted" source, sharing documents within and between process networks, or even creating new automation programs and process files internally, file transfers remain a necessary cog in the industrial machine.

While there's a lot to say about network-based threats, as critical infrastructure operators grow more sophisticated and continue to improve network security measures, the need to move documents, patches, control programs and other files to disconnected workstations and workgroups has increased. There has been a definite increase in attacks that specifically target Operational Technology (OT), as well as increased awareness of such attacks due to broad news coverage of Industroyer, TRITON, Havex, Ekans, USBCulprit, and more. As the second most prevalent attack vector into industrial control and automation systems, USB devices continue to play an important role in these types of targeted attacks.

In context of these USB security concerns and continued advancements in targeted attacks that rely on USB, researchers from Honeywell's Industrial Cybersecurity Global Analysis, Research, and Defense (GARD) team once again analyzed USB usage and behavioral data collected from production sites. This report shares findings from this new research, and identifies emerging trends from the original Honeywell Industrial USB Threat Report. As with the first report, the focus here remains on real threat activity observed from real industrial operations. By analyzing real threats that have been actively detected on removable media that were specifically destined for OT environments, we gain valuable insight into this unique vector. Note that there are also many threats posed by malicious USB devices other than removable media. While significant, these threats are not covered here.

A glossary of terms used in this report is offered at the end of this document.

METHODOLOGY

1

USB usage and behavioral data was analyzed by the Cybersecurity GARD Threat team, using a proprietary and highly cultivated threat detection and analysis engine (the GARD Threat Engine).

While the GARD Threat Engine is used across multiple Honeywell Industrial Cybersecurity products and services, the data for this report was limited to those threats detected by Honeywell's USB security platform: Honeywell Secure Media Exchange (SMX). SMX analyzes USB devices as they are actively used in industrial facilities, providing a highly focused view of critical infrastructure USB activity.

All data collected from SMX, and all data from GARD is anonymous with no personally identifiable information (PII), and only a sample set of all SMX data collected over a 12 month period was analyzed. Due to concerns of confidentiality, no details concerning the collection points have been provided.

Industries represented include Oil and Gas, Energy, Food, Chemical, Shipping, Buildings, Aerospace, Manufacturing, Pulp and Paper, and other industrial facilities. No detailed correlation to region, nor detail by industry, has been provided here, in an effort to further preserve data anonymity. Data was collected from over 60 countries across North America, South America, Europe, the Middle East, and Asia. This sample set represents only files actively carried into production control facilities via USB removable storage devices, during normal day-to-day operations. The data represents those files that were detected and blocked.

KEY FINDINGS

2

USB REMAINS A TOP THREAT VECTOR

In the first USB Threat Report, nearly half (44%) of the locations studied had detected and blocked at least one malicious or suspicious file that represented a security issue. That has increased slightly over time, with 45% of locations blocking at least one threat. This reaffirms that USB remains a significant vector for OT threats. It is almost inevitable that, over time, some threat will find its way onto USB removable media. While this may seem obvious, it is important to keep this in mind when considering the types of threats detected, and the potential impact that they could have on industrial facilitates and critical infrastructure.

USB-BORNE MALWARE: A HIGH-POTENCY THREAT

As before, the volume of malware discovered on USB removable media was a small fraction of the total sample size. This is likely due to the increasing storage volume of removable media devices, which are now able to store enormous amounts of total data. The amount of malware discovered, therefore, remains statistically small overall.

However, the impact of the malware found increased significantly since the first report even if the overall concentration of malware remained steady. In 2018, 14% of total threats detected were known to have been developed specifically to target industrial systems, leveraging a specific vulnerability in industrial devices or protocols. This dropped slightly to 11%. However, a staggering 59% of total threats in our latest study had the ability to impact industrial control and process automation systems, up from just 26%. This directly correlates to the increase in ransomware, which was up from 7% to 17%. Ransomware was not considered "OT specific" unless it specifically targeted an industrial device or protocol, and thus did not contribute to the 11% figure. However, the increase in ransomware seen in OT indicates that industrial corporations are being targeted by ransomware, even if the ransomware itself is not OT-specific. If we include ransomware, the rate of threats targeting OT actually doubles from 16% to 28%.

HONEYWELL CYBERSECURITY RESEARCH REVEALS THE RISK OF USB THREATS TO INDUSTRIALS HAS EFFECTIVELY DOUBLED

The increase in ransomware seen in OT indicates that industrial corporations are being targeted by ransomware, even if the ransomware itself is not OT-specific. If we include ransomware, the rate of threats targeting OT nearly doubles, from 16% to 28%.

OF THE THREATS BLOCKED

59%

Potential to cause major disruption in ICS (up from 26%)

28%

Targeted ICS (including ransomware) (up from 16%)

19%

Designed to exploit USB (up from 9%)

15%

Are well-known threats (No Change)

HIGH CONCENTRATION OF USB-SPECIFIC THREATS

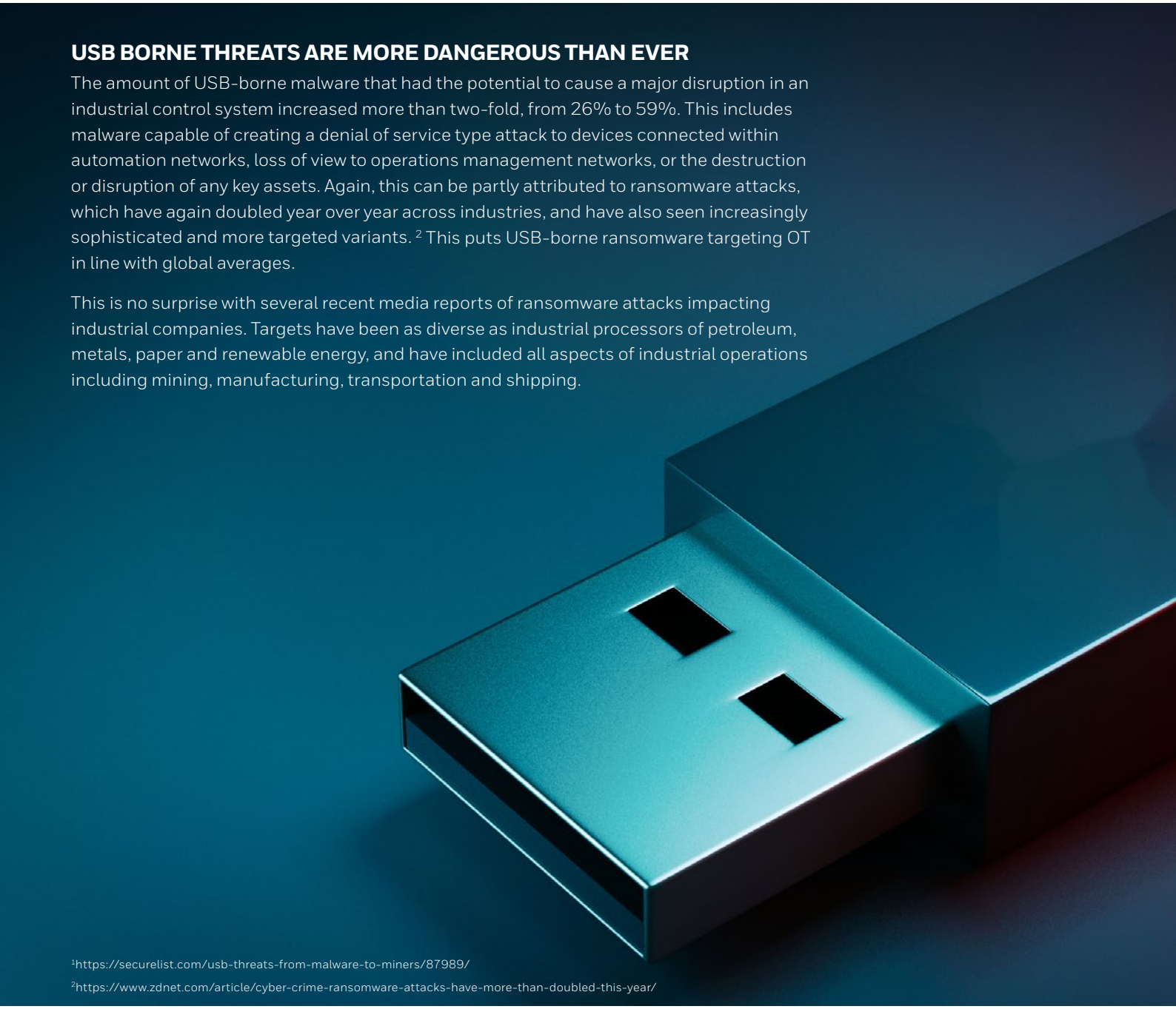
An increasing number of threats found on USBs had removable media in mind. Of the sample analyzed, 19% specifically used USB for infection or propagation. This is more than twice as many as discovered in the initial USB Threat Report, which found just 9% of threats were specifically crafted to leverage USB. A report from Kaspersky Labs in 2018 showed an increase in USB-borne malware vs Web-borne malware, based on an examination of all threats among internet-connected computers in typical IT environments. That ratio began at 1:42, and narrowed to 1:22 in 2018. [1] In comparison, Honeywell's 2018 USB Threat Report, which focused exclusively on the USB vector into OT, found a 1:11 ratio (9%) in 2018, narrowing even further to 1:5 (19%) — approximately twice as prevalent as in IT.

This is an indication that USB devices are an increasingly popular vector for malware infection and propagation, and even more so in OT versus IT. This poses a significant threat against industrial environments, which depend on USB removable media for regular operations. One can easily infer that this is intentional, and that the dependence on removable media in these environments represents a growing vulnerability against such attacks.

USB BORNE THREATS ARE MORE DANGEROUS THAN EVER

The amount of USB-borne malware that had the potential to cause a major disruption in an industrial control system increased more than two-fold, from 26% to 59%. This includes malware capable of creating a denial of service type attack to devices connected within automation networks, loss of view to operations management networks, or the destruction or disruption of any key assets. Again, this can be partly attributed to ransomware attacks, which have again doubled year over year across industries, and have also seen increasingly sophisticated and more targeted variants. [2] This puts USB-borne ransomware targeting OT in line with global averages.

This is no surprise with several recent media reports of ransomware attacks impacting industrial companies. Targets have been as diverse as industrial processors of petroleum, metals, paper and renewable energy, and have included all aspects of industrial operations including mining, manufacturing, transportation and shipping.



[1] https://securelist.com/usb-threats-from-malware-to-miners/87989/

[2] https://www.zdnet.com/article/cyber-crime-ransomware-attacks-have-more-than-doubled-this-year/

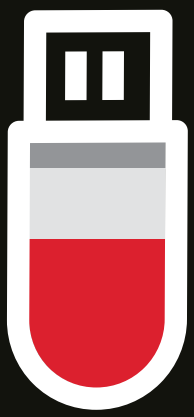
THREAT PATTERNS APPEAR UNIQUE TO OT

Comparing the threats found on USB removable media that are exclusively entering OT facilities – the threats covered in this report – to other studies on USB borne malware, we see distinct differences. For example, in a 2018 report from Kaspersky researchers show that in traditional IT markets, about 9% of USB-borne malware consisted of cryptocurrency mining. [3] In Honeywell's 2018 report, we found that number to be only 4%, and it increased only marginally to 6% since then. This makes sense considering the target environments. Currency mining is lucrative in Enterprises, where large networks and high powered datacenters are attractive targets. OT environments, on the other hand, tend to be isolated and often built from low-powered, legacy infrastructures. Fewer nodes with far less compute power makes for poor mining. So what types of threats do we see targeting OT? The largest increase is clearly in the area of ransomware, which increased from 7% to 17%. The most prevalent threats, however, involved RATs and backdoors, which took the lead at 34% (up from 32% in 2018) and Droppers, which tied for second at 17% (up from 12%). This makes logical sense: in industrial environments, where network access is difficult, gaining a foothold via USB to then establish remote access and download new malware is a sound strategy for an attacker. While ransomware can be effective via USB, establishing a persistent backdoor with command and control, more coordinated attacks can be attempted in these otherwise elusive environments.

ARE USB BORNE THREATS TARGETING OT SYSTEMS DIRECTLY?

If the threats are targeted against OT, why a decrease in OT-targeted threats (from 16% to 11%)? It's partly to do with how industrial-targeted threats were originally defined in the 2018 USB Threat Report: we use the term to describe those threats designed specifically to infect or manipulate OT devices or systems – such as Stuxnet altering process logic to cause physical damage, or TRISIS manipulating industrial safety systems. However, that doesn't mean that other types of threats don't target industrial customers or industrial environments specifically. Again, we need to consider ransomware. Ransomware campaigns are known to target specific geographies, demographics, and vertical markets. Simply put, ransomware campaigns focus their efforts where victims are most likely to pay. This is evident in recent increases in healthcare targets during the 2020 pandemic. It is likely that the increase in ransomware on removable media in OT environments is a result of specifically targeting industrial manufacturing and critical infrastructure, which may be seen by ransomware makers as an increasingly lucrative segment. This certainly seems to be the case with Ekans and other recent ransomware threats found in industrial organizations. If we therefore expand our definition of "industrial targeted" to include ransomware, the number of "targeted" threats against OT increases, rather than decreases: from 16% to 28%, or more than one quarter of all detected threats.

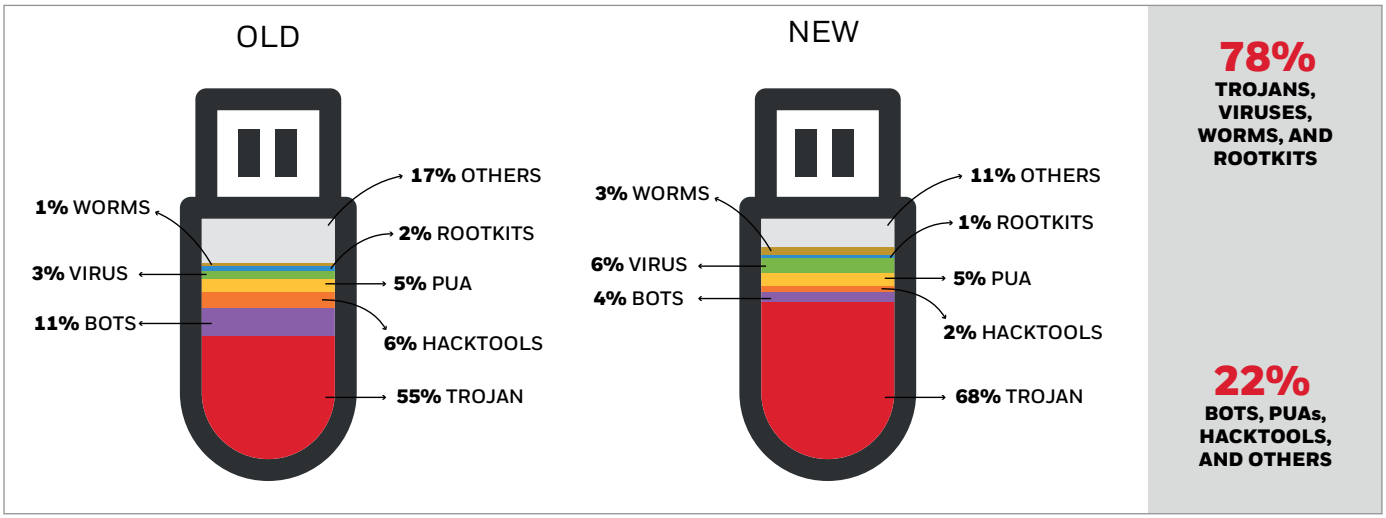
ARE USB TARGETING OT?



16% to 11%
Attacks targeting OT industrial assets (not including ransomware)

16% to 28%
Attacks targeting OT (including ransomware)

26% to 59%
Attacks endangering OT



[3] https://securelist.com/usb-threats-from-malware-to-miners/87989/

IMPROVED HYGIENE, HIGHER RISK

Since the initial threat report, which found an abundance of "junkware" that indicated poor overall USB Hygiene, there was a noticeable reduction in Potentially Unwanted Applications (PUA), non-targeted bots, adware, spyware, and hacktools (39% down to 22%). At the same time, there was an increase in Trojans, worms, rootkits, and viruses (59% up to 78%). Simply put, threat-for-threat, the malware present on USB removable media represents a higher risk than in the past. With 68% of all threats classified as Trojans, and 59% specifically capable of leveraging USB removable media for propagation, it's clear that infections are more about deliberate dissemination and less about accidental exposure.

UP+19%

TROJANS, WORMS AND VIRUSES UP FROM 2018

POTENTIALLY UNWANTED APPLICATIONS (PUAS), NON-TARGETED-BOTS, ADWARE, SPYWARE AND HACKTOOLS DOWN

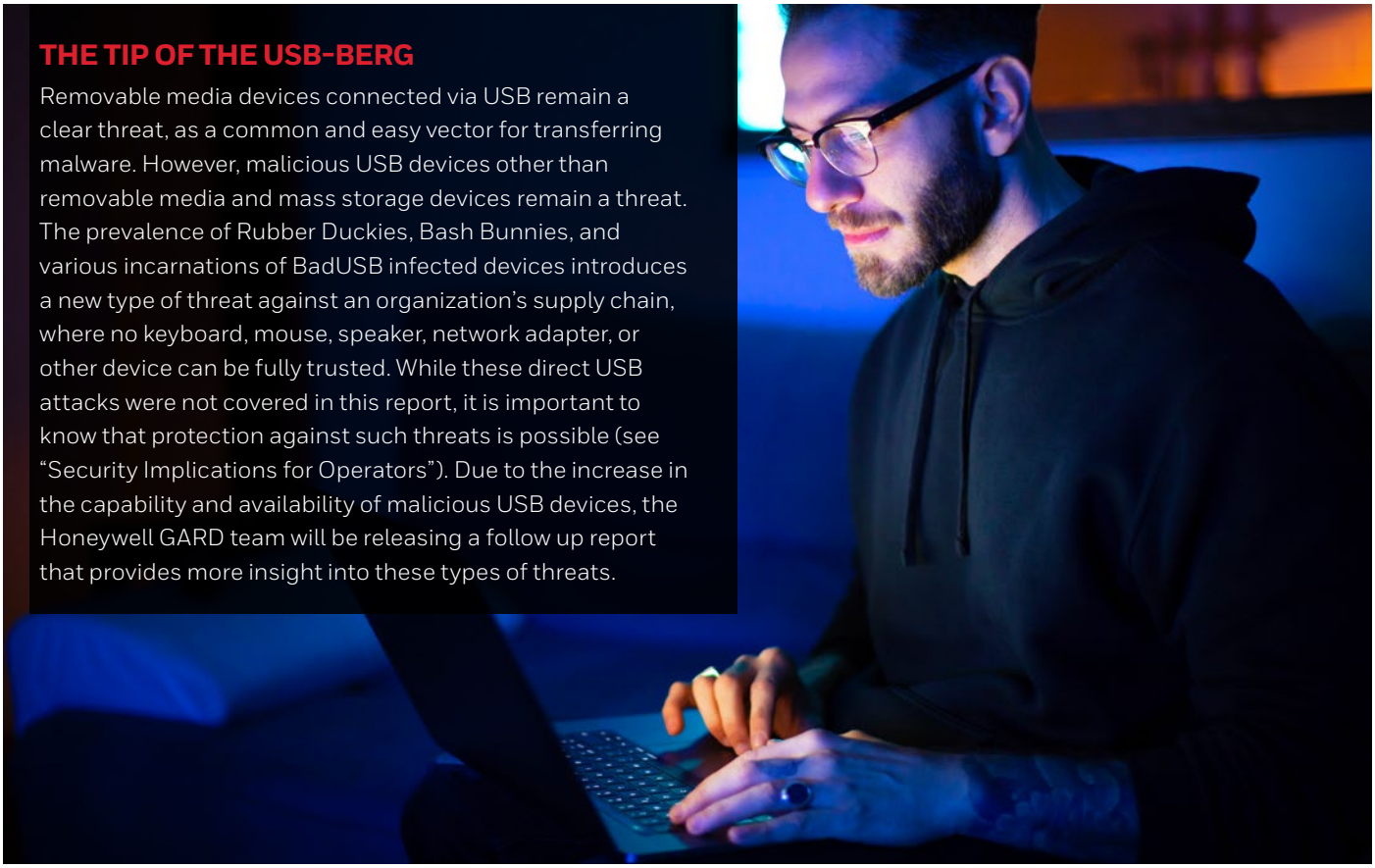
DOWN-17%

WHAT'S IN A NAME?

This report focuses on threats that were successfully detected and blocked from entering industrial facilities. However, there are numerous ways for malware to evade detection, and there is obviously no way to quantify or analyze those threats that weren't detected. One example of evasion includes using filesystem or boot sector irregularities on removable media in order to avoid detection. The GARD research team encountered numerous instances where media contained irregular, illegal, unsupported, or otherwise suspicious file systems and directory structures. It is believed this is mostly indicative of the older technology that is still in use in many industrial environments. Most commodity USB removable storage devices were not built to last, and older media are prone to device errors or failures that cause these same irregularities. While there is no way to differentiate between a legitimate irregularity and an evasion attempt, it is worth mentioning as a potential risk. Especially where USB media is used for critical tasks (such as backups or storage of important files), upgrading to newer, professional grade media is recommended (see 'Security Implications for Operators'). While the good news is that the GARD Threat Engine 'excludes' these files by default (meaning those files are assumed untrustworthy, and therefore not allowed to be accessed), no data is currently captured for these excluded files, preventing further analysis. Additional research is being planned in this area.

THE TIP OF THE USB-BERG

Removable media devices connected via USB remain a clear threat, as a common and easy vector for transferring malware. However, malicious USB devices other than removable media and mass storage devices remain a threat. The prevalence of Rubber Duckies, Bash Bunnies, and various incarnations of BadUSB infected devices introduces a new type of threat against an organization's supply chain, where no keyboard, mouse, speaker, network adapter, or other device can be fully trusted. While these direct USB attacks were not covered in this report, it is important to know that protection against such threats is possible (see "Security Implications for Operators"). Due to the increase in the capability and availability of malicious USB devices, the Honeywell GARD team will be releasing a follow up report that provides more insight into these types of threats.



CATCHING MISSED MALWARE

3

Once again, we cross-checked all threats against a variety of commercial anti-malware software solutions, in order to test the efficacy of Secure Media Exchange and the GARD Threat Engine.

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.

This is consistent with the original findings from the 2018 USB Threat Report. Interestingly, it was noted that in several cases a particular threat was only detected by one or two less-known software solutions. Narrowing the results to the anti-malware vendors (based on market share) with a larger presence in OT markets, we found that 20% of the threats analyzed went undetected, up from 11% in the previous report. With a higher prevalence of newer threats (5% being less than one week old), and clear indications of high-impact, targeted threats against industrials originating from USB removable media, this remains a concern. Many industrial organizations update anti-virus signatures less frequently, due to the limited availability of maintenance windows where such updates can occur, which can further increase the risk of depending solely on commercial AV scanning.

SMX improves detection performance using the GARD Threat Engine, which includes a variety of advanced threat detection and threat intelligence technologies and methods. While these report findings indicate that The GARD Threat Engine is performing well, the severity of the threats discovered warrants the use of additional security measures for true defense-in-depth (see “Security Implications for Operators”).

SECURITY IMPLICATIONS FOR OPERATORS

4

- Evidence indicates that new threat variants are being introduced more quickly, specifically via USB, and specifically targeting industrials. To this end, existing controls should be re-examined, and patch cycles should be re-evaluated in an attempt to close the Mean Time to Remediation (MTTR). External controls to provide real-time detection and protection of key systems should be considered, as well as integrated monitoring and incident response procedures. For more information on closing the MTTR gap in OT environments, please refer to Responding to Incidents in Industrial Control Systems: Identifying Threats/ Reactions and Developing the IR Process.
- 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 seeming widespread belief that USB drives are dangerous, and despite the prevalence of corporate USB usage policies, the data provides ample evidence that the threat of USB-borne malware is still increasing.
- 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.
- Ransomware is an increasingly 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
- Security upkeep remains important: Anti-virus software deployed in process control facilities needs to be updated daily to be effective. Even then, additional protection is recommended.
- Patching and hardening of end nodes remains 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. Hardening of OT systems is also a key contribution to improving incident MTTR.
- Legacy USB devices pose a risk. In addition to potential vulnerability to BadUSB or other firmware corruption, older USB devices are susceptible to errors or corruption of the boot sectors and filesystems that can impact the reliability of older operating systems and even introduce new vulnerabilities – putting data and system integrity at risk. Consider upgrading removable media to newer USB3.0 or later. For maximum protection, choose brands that offer signed and validated firmware.

CONCLUSION
MORE RESEARCH IS NEEDED

5

Since the last USB Threat Report, there has been an increase in the frequency and the impact of USB-borne threats.

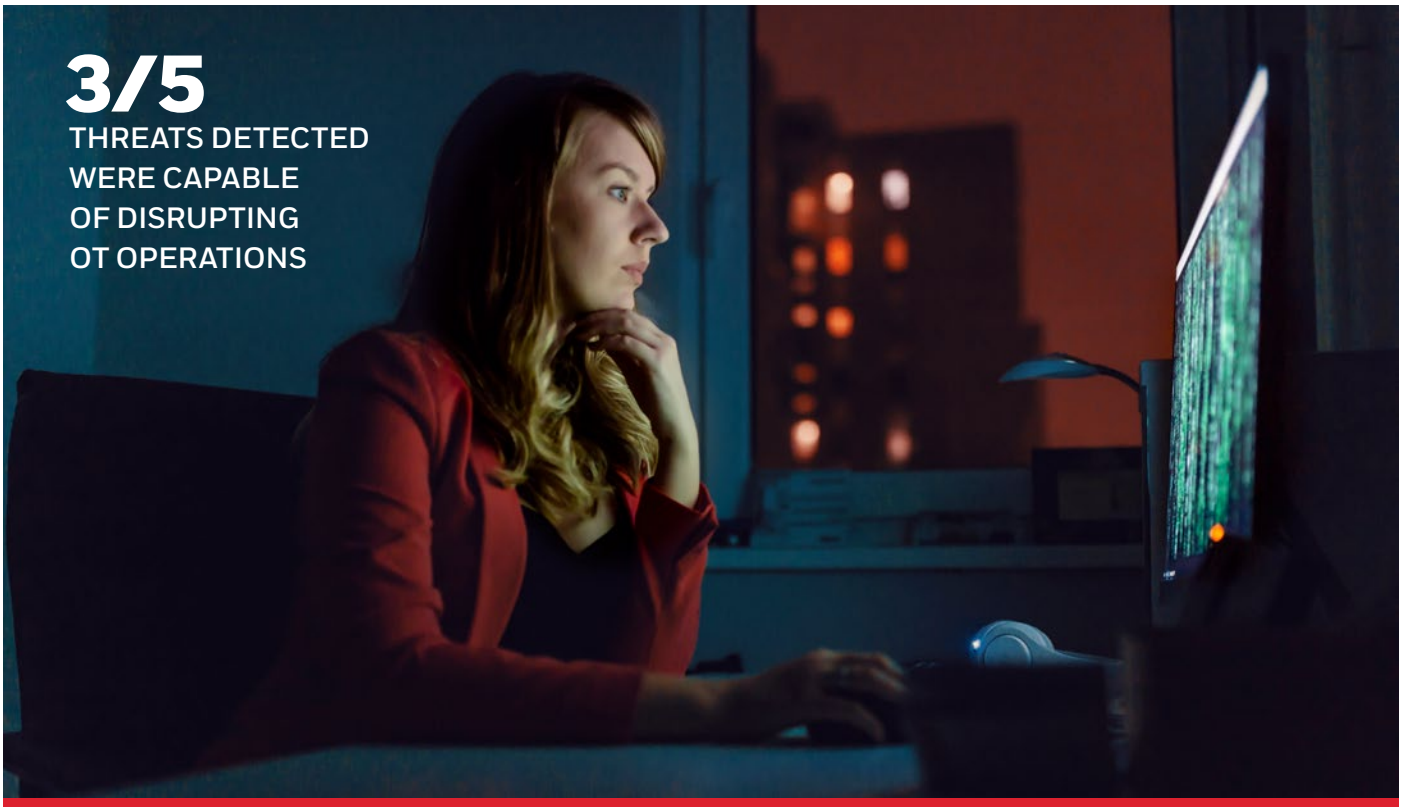
Early indicators that USB removable media are being used as a deliberate attack vector into OT have been reinforced by an increased detection rate of USB-specific malware, as well as continued detection of malware that specifically targets industrial control / OT organizations. While the overall amount of malware remained relatively small, the overall exposure rate was even higher – with 45% of the SMX gateways analyzed blocking at least one malicious file (up slightly from 44%). The risk of potential disruption to ICS has also increased, from 26% to nearly 3 out of every 5 threats (59%) detected being capable of disrupting OT operations.

This tells us that USB removable media is not only a real threat, but that the threat is increasing. However, dedicated USB security research is still uncommon, and many organizations lack a clear strategy to improve defenses against these types of attacks.

This report shares Honeywell USB security research findings in an effort to foster that research, and to advance industry collaboration, in hopes of lowering cyber attack risk to industrial operations worldwide.

"Being able to quantify actual threats seen over a very specific vector proves what everyone already suspected – that USB-borne malware continues to be a major risk for industrial operators. What's surprising is that we're seeing a much higher density of significant threats that are more targeted and more dangerous. This isn't a case of accidental exposure to viruses over USB, this is a trend of using removable media as part of more deliberate and coordinated attacks."

– ERIC KNAPP,
DIRECTOR OF CYBERSECURITY RESEARCH AND ENGINEERING FELLOW, HONEYWELL CONNECTED ENTERPRISE



HONEYWELL CYBERSECURITY RESEARCH REVEALS THE RISK OF USB THREATS TO INDUSTRIALS HAS DOUBLED

GLOSSARY

6

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.

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.

Cryptocurrency Mining / Crupto-mining
Cryptomining malware, or cryptocurrency mining malware or simply cryptojacking, is a relatively new term that refers to software programs and malware components developed to take over a computer's resources and use them for cryptocurrency mining without a user's explicit permission.

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.

EKANS
EKANS, also referred to as "Snake", is a new ransomware threat that has characteristics specific to industrial processes, and is largely considered to be the first ransomware variant built specifically to target ICS.

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.

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 Cybersecurity 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 Cybersecurity technical solution developed by Honeywell to lower the risk of USB-borne threats. For more information, visit https://www.hwll.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.

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'S GLOBAL ANALYSIS, RESEARCH AND DEFENSE TEAM FOR OT CYBERSECURITY

Honeywell 's Global Analysis, Research, and Defense team (GARD) is dedicated to OT focused cybersecurity research, innovation, and integration. As part of Honeywell Forge Cybersecurity, GARD leverages data curated from 7 Honeywell cybersecurity research centers, and from over 5,000 deployments in over 65 countries – to provide OT threat analysis and threat detection. Proactive threat research, mining, hunting and other techniques can help ensure that targeted OT threats are detected early.

Honeywell Forge Cybersecurity better protects industrial assets, operations and people from digital-age threats. With more than 15 years of OT cybersecurity expertise and more than 50 years of industrial domain expertise, Honeywell combines proven cybersecurity technology and industrial know-how to maximize productivity, improve reliability and increase safety. We provide innovative cybersecurity software, services and solutions to better protect assets, operations and people at industrial and critical infrastructure facilities around the world. Our state of-the-art Cybersecurity Centers of Excellence allow customers to safely simulate, validate and accelerate their industrial Cybersecurity initiatives.

For more information

To learn more, visit www.becybersecure.com or contact your Honeywell Account Manager, Distributor or System Integrator.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, GA 30308
www.honeywell.com

WP-20-16-ENG | 07/20
© 2020 Honeywell International Inc.

THE FUTURE IS WHAT WE MAKE IT

Honeywell