HONEYWELL
FORGE

INDUSTRIAL CYBERSECURITY USB THREAT REPORT 2022

Threats designed for USB exploitation rise to 52%. Growth indicators slow, but threat levels remain dangerously high.

Research Report

OVERVIEW

By looking at a very specific vector into industrial automation environments, we get a unique opportunity to analyze the real malware threats that industrial organizations face.

This is important because there are only a few actual vectors into OT (Operational Technology) environments: the network, limited to specific information conduits between operational and business networks; physical access by authorized users; and supply chain through which hardware and software enters a mill, plant, refinery, or other industrial automation facility.

Removable media falls into two of these categories: *physical access* (thumb drives and other media physically carried into a facility); and the *supply chain*. This report focuses specifically on *malware* (intrusive software) found on USB storage devices used to carry files into, out of, and in between industrial facilities.

The results of the Honeywell Industrial Cybersecurity USB Threat Report are based on malware detected and blocked by technology deployed globally by Honeywell. All data is anonymous, and therefore no correlation can be made to specific organizations, industries, or geographic regions. However, all data is derived from production OT facilities, presenting a unique glimpse at the types of malware threats facing industrial environments via USB removable media.

Note: Malicious USB devices and peripherals crafted specifically to attack computers via the USB interface, while increasingly popular and highly effective, are not included in this report (please refer to the Honeywell USB Hardware Attack Platforms Report).

THE CHALLENGE

Now in its fourth year, the Honeywell Industrial Cybersecurity USB Threat Report has shown a clear trend: threats continue to become more prominent and more potent.

- Threats designed to propagate over USB or specifically exploit USB for infection rose to 52% from 37%.
- Threats designed to establish remote access capabilities remained steady at 51%.
- Threats capable of causing loss of control or loss of view increased to 81%, up from 79%.

Previous versions of this report showed massive increases, even doubling in many cases, this year the growth of many indicators slowed. These more moderate increases indicate the level of threats utilizing this vector may have plateaued – **although they do so at dangerously high levels**.

THREATS

Designed for USB	**52%**
Disruptive Against OT	**81%**
Industrial Specific	**32%**
Remote Access	**51%**

METHODOLOGY

USB usage and behavioral data was analyzed by Honeywell's Cybersecurity Global Analysis, Research, and Defense **(GARD)** team, using a proprietary and highly cultivated threat detection and analysis system called 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).

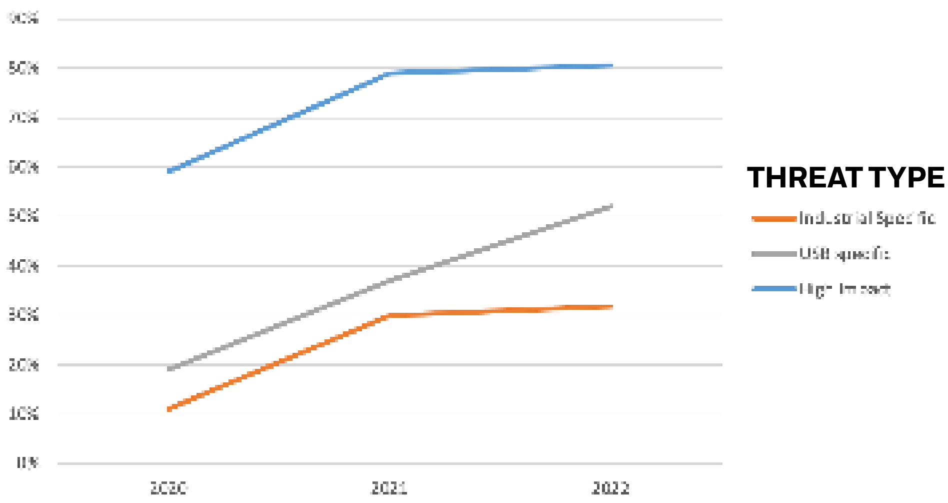
Honeywell SMX analyzes USB devices as they are actively used in industrial facilities, providing a highly focused view of industrial USB activity.

While this report is based on aggregated data from Honeywell SMX and is fully anonymized, the 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 all critical infrastructure sectors defined by the Cybersecurity & Infrastructure Security Agency (CISA).

As mentioned, findings are limited to malware that has been detected and blocked. As no malware detection technology is 100% effective, it is therefore possible that additional threats were not detected, and as a result not included in this report.

YEAR OVER YEAR TRENDS

Growth indicators slow, but threat levels remain dangerously high.



THREAT TYPE	2020	2021	2022
INDUSTIRAL SPECIFIC	11%	30%	32%
USB SPECIFIC	19%	37%	52%
REMOTE ACCESS		51%	51%
HIGH IMPACT	59%	79%	81%

KEY FINDINGS

Overall, the threat of **USB-borne malware** continues to be a serious concern. Threats capable of propagating over USB, or specifically exploiting USB media for initial infection, rose from 19% in 2019 to just over 37% in 2020, to 52% in 2021 – representing a pattern of slowing (yet still concerning) growth found throughout most indicators.

Of the threats seen, **Trojans** still dominated, once again comprising 76% of the malware detected. Malware capable of providing remote access or remote control also remained steady at 51%. This solidifies our suspicion that adversaries are deliberately leveraging USB removable media as an initial **attack vector**, at which point they will attempt to establish remote connectivity to download additional payloads, exfiltrate data, and establish command and control.

Combined with a corresponding increase in threats targeting industrials (from 30% to 32%), this again validates the theory that USB removable media are being used to penetrate the **air-gapped** environments found in many industrial/OT environments.

HIGHER LIKELYHOOD OF DISRUPTION

While these findings do not prove a concerted intention to bypass airgaps in industrial systems, it does highlight an increased capability to do so. In addition, looking at the malware samples validated another trend that first surfaced last year. The number of threats designed specifically to target industrial control systems also increased slightly year over year, up from 30% to 32%, while at the same time the malware was more capable of causing a disruption to industrial control systems, up from 79% to 81%.

RECOMMENDED SECURITY ACTIONS FOR OPERATORS

- **A clear USB security policy must be established.** Evidence indicates USB removable media is intentionally used as an initial attack vector into industrial control / OT environments. As such, technical controls and enforcement must be established to better secure USB media and peripherals.
- **Close the Mean Time to Remediation (MTTR).** Evidence continues to indicate 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 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.
- **Additional scrutiny should be placed on files, documents, and other digital content.** Inspection and detection-based controls are necessary for the primary vectors into and between protected industrial facilities (e.g., removable media, network connections), to improve your ability to prevent the introduction and propagation of content-based malware.
- **Outbound network connectivity from process control networks must be tightly controlled** and be enforced by network switches, routers and firewalls. Threats crossing the air gap via USB are used to establish a toe hold into industrial systems, establishing backdoors and remote access to install additional payloads and establish remote command-and-control.
- **Security upkeep remains important.** Anti-virus software deployed in process control facilities needs to be updated daily. Even then, a layered approach to threat detection that includes OT-specific threat intelligence is strongly recommended for maximum efficacy. Due to the large percentage of threats encountered in OT environments that were able to evade detection by traditional anti-malware software, it is critical that anti-malware controls are kept current in order to be effective.
- **Patching and hardening of end nodes is necessary** due to the extent of threats that are capable of establishing persistence and covert remote access to otherwise air-gapped systems. Hardening of OT systems is also a key contribution to improving incident MTTR.

CONCLUSION
ACTIVE USB CYBERSECURITY CONTROLS ARE REQUIRED

For the fourth year in a row, the threats seen attempting to enter industrial/OT environments have continued to increase in sophistication, frequency, and in their potential risk to operations. USB-borne malware is clearly being leveraged as part of larger cyber attack campaigns against industrial targets. Adaptations have occurred to take advantage of leveraging the ability of USB removable media to circumvent network defenses and bypass the air gaps upon which many of these facilities depend on for protection. Continued diligence is necessary to defend against the growing USB threat, and strong USB security controls are highly recommended.

GLOSSARY

Air Gap

An air gap refers to the purposeful absence of digital connectivity between a computing environment and any outside or untrusted network, such as the internet. In industrial controls, there is typically an approximation of an air gap that separates operational and automation systems ("OT") from business systems ("IT"). While absolute air gaps are rare due to the increasing need for digital communications between business and operational systems, the term is still widely used to refer to the layer of strict network access policies, logical segmentation, and security controls around OT environments.

Attack Vector

An attack vector is any potential path by which a cyber adversary might attempt to gain access to a computer network or system.

Backdoor

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.

Command and Control, C2

Command and Control typically refers to servers used by cyber adversaries that provides the attacker with the ability to communicate with and send commands to a compromised system, providing control over that system.

Cyber Attack Campaigns

A set of coordinated cyber activities carried out by a cyber adversary, towards a common objective, is often referred to as a cyber attack campaign. Campaigns typically utilize multiple attack techniques over time. Campaigns are coordinated efforts, and sometimes implicate threat actors from nation states, crime syndicates or other organized cyber adversaries.

Early Threat Detection, Early-day Threat, ETD

Early Threat Detection is a service offered as part of Honeywell's GARD threat detection offerings. Early Threat Detection refers to the curation of threat and incident information from Honeywell as well as public- and private-sector partners, with the intent of providing detection of newly emerging threats as quickly as possible.

GARD

GARD refers to the Honeywell Global Analysis Research and Defense threat detection service, which provides advanced threat detection and response capabilities to supported Honeywell cybersecurity products.

Industrial Control Systems, ICS, Industrial Control and Automation Systems

Industrial Control Systems refer to the systems, devices, networks, and controls used to operate and/or automate an industrial process.

Mean Time to Remediation, MTTR

The Mean Time to Remediate refers to the amount of time required for an organization to react and recover from an identified cyber threat or incident. In OT, MTTR typically extends beyond simple computer system and network recovery, to fully operational.

Operational Technology, OT

Operational Technology (OT) is analogous to Information Technology (IT), referring to the underlying technology used in ICS environments. While many of the general computing platforms used in ICS share common hardware, operating systems, and networking technology, OT systems are used in fundamentally different ways to support industrial automation and control, and therefore represent a unique challenge in terms of cybersecurity.

Payload

In general computing a "payload" refers to the part of a digital communication that is the actual content or message. A malicious payload, or the payload delivered by a cybersecurity threat, refers to software that performs a malicious activity. Newer and more sophisticated malware will typically operate in a modular fashion, where specific payloads can be used to execute specific tasks in a cyber attack campaign.

Remote Access, RAT
Remote access refers to the connectivity to a computer system or network from a remote location. In the context of cyber threats, remote access typically refers to backdoors or RATs (Remote Access Trojans or Remote Access Toolkits), which are designed to establish unintended network access to a cyber adversary.

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

Trojan
A "trojan" is any malware designed to trick a user into executing it. Typically, this is done by masquerading as legitimate software, or by embedding malicious code or scripts into everyday documents.

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.

USB Attack Platforms, UAPs
USB Attack Platforms refer to attack platforms that are designed to leverage the USB standards via software and hardware. Typically consisting of a maliciously designed or modified USB device that is able to leverage standard USB interfaces for infiltration and exploitation. Examples include HID Attacks, rogue access points, electrical attacks, and many more.

USB-borne Malware
Malware that is transported or propagated via a USB removable media device. This typically consists of infected files that are saved to a portable hard drive, either by a human user or by other malware. Once on a USB drive, the malware can spread to other computers via that drive.

USB Removable Media
USB Removable Media typically refers to data storage devices that connect using the USB standard. Often referred to as flash drives, thumb drives, USB sticks, et al., the most common form of USB Removable Media utilizes solid state storage (i.e., "flash") and connect to USB type-A interfaces using the USB standard "USBStor" device classification. However, the USB standard is diverse and other storage device types are available, and non-flash USBStor devices also exist.

Worm, Wormable
A computer worm is a standalone malware computer program that is able to self-replicate by spreading to and infecting other computers. As malware continues to evolve, it becomes harder to strictly classify a particular malware into a single category (e.g., a trojan might also be able to self-replicate).

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

Proactive threat research, mining, hunting and other techniques can help ensure that targeted OT threats are detected early. Honeywell 's Global Analysis, Research, and Defense team (GARD) is dedicated to OT focused cybersecurity research, innovation, and integration. As part of Honeywell OT Cybersecurity, GARD leverages data curated from 7 Honeywell cybersecurity research centers, and from over 6,000 deployments in over 65 countries – to provide OT threat analysis and threat detection.

Honeywell OT Cybersecurity is a Honeywell business dedicated to better protecting 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.

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written consent. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. The quantified product benefits referenced are based upon several customers' use cases and product results may vary. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion. All product screenshots shown in this document are for illustration purposes only; actual product may vary.

Honeywell® and Honeywell Forge®
are registered trademarks of
Honeywell International Inc.

Other brand or product names are
trademarks of their respective owners.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.honeywellforge.ai

© 2022 Honeywell International Inc.

Honeywell