HONEYWELL GARD

USB THREAT REPORT 2024

Honeywell

TABLE OF CONTENTS

Executive Summary 2

Year over Year Observations Concerning the Types of Malware Discovered 2

Analyses of Content-Based Malware 3

Key Observations 3

Top Exploits by CVE 4

Analysis of Attack Techniques 5

What It Means 6

Multi-Stage, Disruptive Malware 6

Overall Malware Frequency Continues to Rise 6

Security Implications for Operators 7

Notable Threats 7

Conclusion: Active USB Cybersecurity Controls Are Increasingly Important; More Inclusive Document Management and Control Is Critical 8

Methodology 9

Glossary 10

About Honeywell's Global Analysis, Research and Defense Team for OT Cybersecurity 12

EXECUTIVE SUMMARY

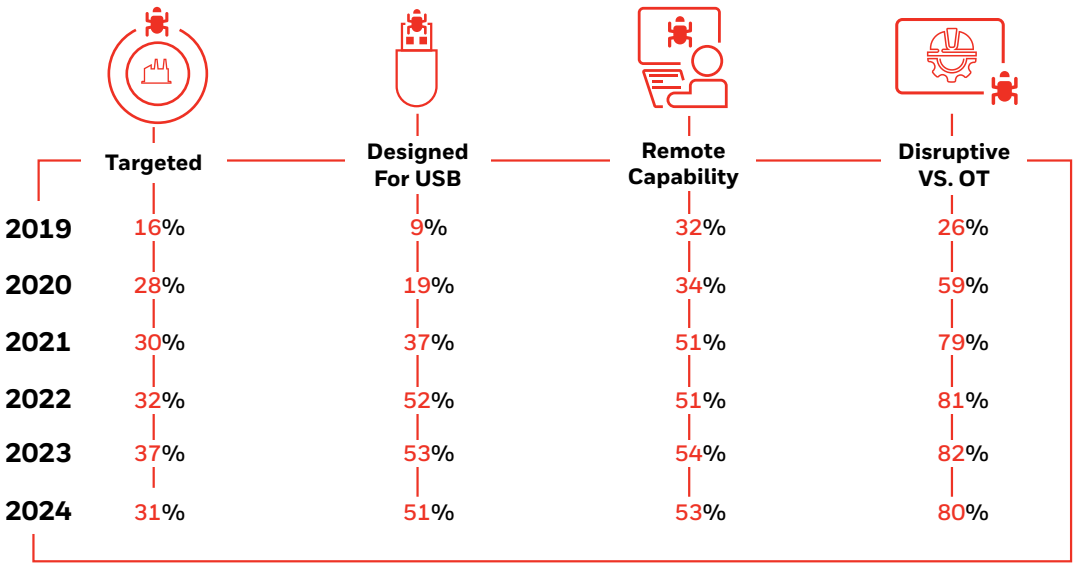
Honeywell's Global Analysis, Research and Defense (GARD) team has been tracking and analyzing USB-borne malware for six consecutive years. This year there are several interesting new observations to make concerning the types of malware discovered, how they operate and what that implies about the sophistication of the adversary. For example, there are indications that adversaries have a strong understanding of industrial environments and how they operate as well as indications that show prominent malware capabilities reflecting "living off the land" (LotL) strategies that have been observed in recent global cybersecurity incidents.

While the threat activity rose quickly in the first few years, in the context of both quantity and capability, it has plateaued in the last few years. This year's analysis again reaffirms the severity of USB-borne malware and the risk it poses to industrial control environments, although these metrics don't tell us anything new beyond this:

- The majority of blocked malware is still capable of causing a significant impact to process control, including loss of view, loss of control or system outage.
- The high prevalence of remote capability, combined with an apparent focus on industrial targets, once again implies that the malware analyzed is intentionally leveraging removable media to cross-secure network perimeters (a.k.a. the "air gap").

The research indicated that adversaries have a strong understanding of industrial environments and how they operate. For the fifth year in a row, the threats seen attempting to enter industrial/OT environments have continued to increase in sophistication, frequency, and the potential risk to operations. USB-borne malware is clearly being leveraged as part of larger cyberattack campaigns against industrial targets

YEAR OVER YEAR OBSERVATIONS CONCERNING THE TYPES OF MALWARE DISCOVERED



The 2024 Honeywell USB Threat Report finds that USBs are increasingly used in targeted attack campaigns

Together, these metrics support the belief that USB-borne malware is intentionally leveraged as part of a coordinated attack campaign against industrial targets, including capabilities that can cause loss of view and/or control.

In 2023, the GARD team began tracking additional metrics to help shed more light on this trend, and this year we are able to further support that theory. By looking closer at malware capabilities, examining the specific tactics and techniques as defined by the MITRE ATT&CK framework[(1)] and correlating that against known qualities of industrial targets, we can paint a clearer picture of our view of the real threat that USB media poses against industrial control environments.

KEY OBSERVATIONS

Several new observations were made, including:

- A significant portion of blocked malware was content-based, using existing documents and scripting functions maliciously rather than attempting to exploit novel vulnerabilities. Among the specific exploits that were found, the majority focused on document and package vulnerabilities (e.g., word processing documents).
- A significant portion of ATT&CK techniques are aligned with observations of real-world cyber-physical attack campaigns, and a shift toward LotL strategies, focusing heavily on OLE and command-line execution techniques.
- In addition to expected target platforms (e.g., Windows), there was an increase in Linux and other target platforms, many of which are often used specifically by purpose-built devices in many industrial facilities, particularly in the areas of asset tracking, quality control, production management and other areas of the industrial supply chain.

Together, this indicates that adversaries are well-educated in industrial process control, supply chains and the day-to-day operations of industrial facilities.

Our analysis of our data resulted in several findings.

Approximately **20%** of all malware analyzed was classified as content based.

Over **13%** of all malware blocked specifically leveraged the inherent capabilities of common documents such as Word documents, spreadsheets, scripts, etc.

An additional **2%** of malware specifically targeted known vulnerabilities in common document formats, and an additional **5%** specifically targeted the applications used to modify and create these file types.

ANALYSES OF CONTENT-BASED MALWARE

Our analysis of our data resulted in several findings. Approximately 20% of all malware analyzed was classified as content based. Over 13% of all malware blocked specifically leveraged the inherent capabilities of common documents such as Word documents, spreadsheets, scripts, etc. An additional 2% of malware specifically targeted known vulnerabilities in common document formats, and an additional 5% specifically targeted the applications used to modify and create these file types.

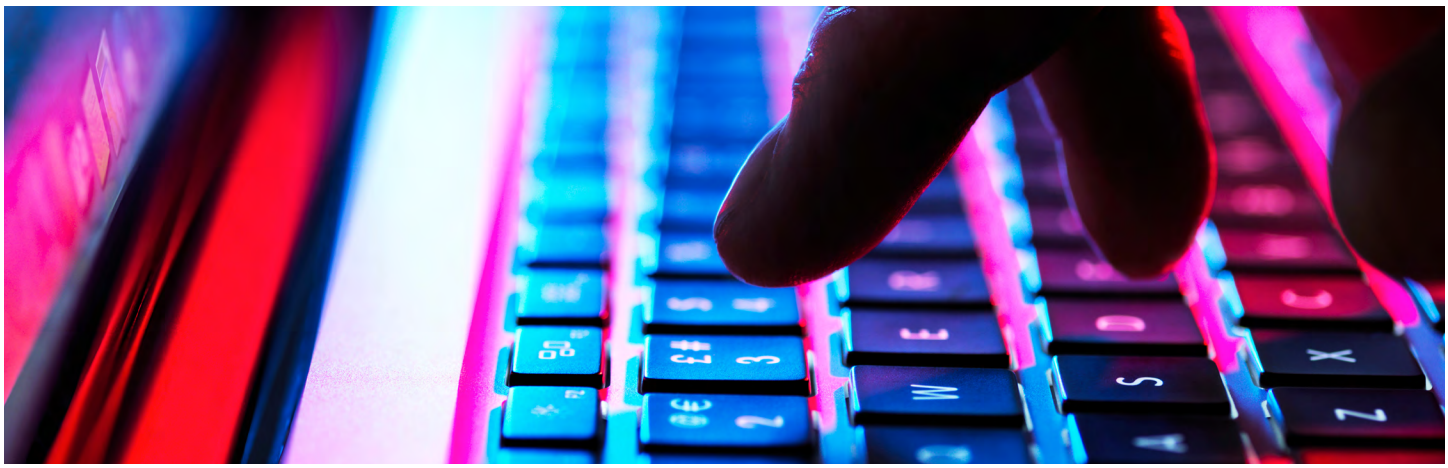
The use of malware designed to infect common document formats and/or exploit the applications used to create and modify those documents makes sense for a USB-borne malware strategy. After all, removable media drives are used specifically for transferring files. In industrial environments, USB drives are often used to transfer files between disconnected or isolated systems.

The presence of both infected documents and malware designed to infect existing documents highlights the need for diligence in document handling within and between sites.

TOP EXPLOITS BY CVE [2]

VULNERABILITY	SCORE	TARGET	DESCRIPTION
CVE-2014-7247	N/A	JustSystems Ichitaro 2008 through 2011; Ichitaro Government 6, 7, 2008, 2009 and 2010; Ichitaro Pro; Ichitaro Pro 2; Ichitaro 2011 Shou; Ichitaro 2012 Shou; Ichitaro 2013 Gen; and Ichitaro 2014 Tetsu.	Arbitrary code execution via a crafted file.
Paragra CVE-2017-11882 Microsoft Office Memory Corruption Vulnerability	**7.8** (CVSSv3)	Microsoft Office 2007 Service Pack 3; Microsoft Office 2010 Service Pack 2; Microsoft Office 2013 Service Pack 1; and Microsoft Office 2016.	Arbitrary code execution.
CVE-2010-2883 Adobe Acrobat and Reader Stack-Based Buffer Overflow Vulnerability	**9.3** (CVSSv2)	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X.	Arbitrary code execution or denial of service via a crafted file.
CVE_2018_0798 Microsoft Office Memory Corruption Vulnerability	**8.8** (CVSSv3)	Equation Editor in Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013 and Microsoft Office 2016 allows a remote code execution vulnerability due to the way objects are handled in memory, a.k.a. "Microsoft Office Memory Corruption Vulnerability."	Arbitrary remote code execution.
CVE-2011-2462 Adobe Acrobat and Reader Universal 3D Memory Corruption Vulnerability	**10** (CVSS v2)	The Universal 3D (U3D) component in Adobe Acrobat and Reader.	Arbitrary code execution or denial of service via a crafted file.
CVE-2016-1019 Adobe Flash Player Arbitrary Code Execution Vulnerability	**9.8** (CVSSv3)	Adobe Flash Player 21.0.0.197 and earlier.	Arbitrary remote code execution or denial of service.
CVE-2012-0158 Microsoft MSCOMCTL.OCX Remote Code Execution Vulnerability	**9.3** (CVSSv2)	MSCOMCTL.OCX in the Common Controls in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4 and 2008 SP2, SP3 and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2 and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0 Runtime.	Arbitrary remote code execution or denial of service via a crafted file.

ANALYSIS OF ATTACK TECHNIQUES



Our analysis of our data also provides a more granular picture of the threat of USB media. We know that USB drives are an established vector into operational technology (OT). We also know a lot about the nature of cyber-physical attacks, based on analysis of previous and ongoing cyber-physical attack campaigns.

- Cyber-physical attacks require extensive knowledge of the target systems, especially concerning the protocols used within control environments and the points managed by those systems. [3]
- Cyber-physical attacks have become less dependent on exploitation techniques, instead leveraging the inherent capabilities of the control environment.[4] This has culminated in recent examples of LotL attacks against energy infrastructure in Ukraine, which solely use the inherent capabilities of the system against it. [5]

From our analysis of ATT&CK tactics and techniques seen on inbound removable media to which we had access, we see:

- Discovery, collection and exfiltration consisted of **36%** of all observed tactics.
- Defense evasion and persistence consisted of **29%** of all observed tactics.
- Credential access and privilege escalation consisted of **18%** of all observed tactics.
- Narrowing the scope solely to the ICS-specific attack tactics within the ATT&CK ICS matric, we see tactics consisting solely of execution **(75%)** and privilege escalation **(25%).**
- The most common execution techniques are scripting, command-line interface and dynamic data exchange using OLE. These accounted for **50%** of execution techniques and **21%** of all observed techniques.

This supports the idea that adversaries targeting industrial operators are focusing less on novel malware or other detectable attack techniques and are instead leveraging existing system capabilities – such as those used in a LotL strategy. By focusing on data collection, obtaining privileged access and LotL execution tactics, an adversary could establish and maintain long-term persistence, with the ability to manipulate the target at any moment, and have significant impact potential.

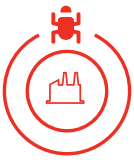
WHAT IT MEANS

DESIGNED FOR USB

Malware that has capabilities to look for and spread via USB removable drives, or where there have been known cyber attack campaigns to distribute the malware via USB.

DISRUPTIVE VS. OT

Malware that has the capability of causing an impact to OT, either through loss of view or loss of control.



TARGETED

Malware that is part of, or associated with, a known campaign that has targeted industrial systems or companies.

REMOTE CAPABILITY

Malware that is intended to establish and/or leverage remote connectivity, typically to a malicious server for purposes of command and control (C2).

MULTI-STAGE, DISRUPTIVE MALWARE

Our analysis indicates that the occurrence of disruptive malware has remained steady at 82%. This means that of the malware detected, the majority of it could cause loss of view or loss of control to industrial control operators. This category of malware includes cyber-physical malware intended to manipulate or disrupt control, ransomware targeting industrial operators and wiper malware associated with industrial attack campaigns.

In the context of the observed techniques, and the correlation between these techniques and those used in recently observed "living off the land" cyber attack strategies, this potential should be concerning to operators, especially operators of critical infrastructures. The malware analyzed is consistently capable of enabling adversaries to "dig in," remain hidden and manipulate the inherent capabilities of target systems at any time. The findings also support the continuing trend of capable and modular malware frameworks that are typically used in multi-stage attacks. This includes malware associated with cyber-physical attack campaigns, including variants of Black Energy, Industroyer and Industroyer 2 malware used in attacks against Ukraine's electricity distribution systems as far back as 2015. [6]

" Our analysis indicates that the occurrence of disruptive malware has remained steady at 82%"

OVERALL MALWARE FREQUENCY CONTINUES TO RISE

The amount of malware detected and blocked, relative to the total amount of files scanned, increased by approximately 33% over the previous year, which in turn was a 700% increase year-over-year. Note that the GARD team does not provide exact statistics about the total number of malicious files found because these types of statistics are far too easy to misinterpret. The amount of malware detected can be influenced by any number of factors, including malware prevalence, detection efficacy, shifts in malware types and behaviors, end-user practices and more. We believe this makes it impossible to correlate the number of files blocked to any specific behavior. However, the 2023 increase was significant enough that the GARD team felt it was noteworthy as a general indication that malware exposure via USB has increased to some degree and that this exposure has remained elevated. The GARD team will begin to track additional data points around malware prevalence in hopes of obtaining more insight in the future.

"The amount of malware detected and blocked, relative to the total amount of files scanned, increased by approximately 33% over the previous year, which in turn was a 700% increase year-over-year. "

SECURITY IMPLICATIONS FOR OPERATORS

- New evidence indicates an awareness of target industrial environments and how they operate, specifically in terms of the target platforms used, the types of documents used and the manner in which files are transferred within these environments.
- New evidence indicates that adversaries are pursuing LotL strategies, combining more sophisticated detection avoidance and persistence techniques with execution techniques that leverage the inherent capabilities of the target systems.
- Evidence continues to indicate that USB removable media is intentionally used as an initial attack vector into industrial control/OT environments. As such, it is recommended that organizations should establish a clear USB security policy, and technical controls and enforcement should be established to improve security for use of USB media and peripherals.
- Evidence continues to indicate that new threat variants are being introduced more quickly, specifically via USB, and that they are targeting industrials. To this end, existing controls should be reexamined, and OT cybersecurity policies and procedures should be reevaluated 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.
- Threats crossing the air gap via USB are used to establish a toe hold into industrial systems, opening backdoors and remote access to install additional payloads and remote command-and-control. Outbound network connectivity from process control networks must be tightly controlled and enforced by network switches, routers and firewalls.
- Security upkeep remains important. 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 current in order to be effective. 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 extent of threats capable of establishing persistence and covert remote access to otherwise air-gapped systems, patching and hardening of end nodes – especially those that are exposed to early-stage attacks – is necessary to improve an organization's ability to prevent eventual breach of process control systems.

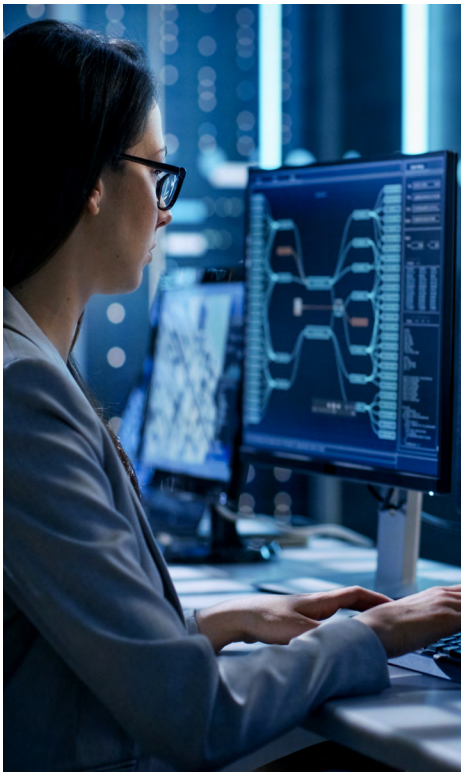
NOTABLE THREATS

With nearly half a billion new malware applications being discovered every day[7], and with 82% of the blocked threats referenced in this report being highly disruptive to OT, it's difficult to single out specific threats as "notable." However, some more interesting findings included:

- Ransomware, including DarkSide, REvil, Sodinokibi, WannaCry, Snake, TeslaCrypt and others, remained prevalent. DarkSide, REvil, Snake (also known as Ekans) and WannaCry are known to target industrial industries including transportation, oil & gas and manufacturing.
- Malware associated with cyber-physical threats, including Stuxnet variants, Triton, Black Energy, Industroyer and Industroyer 2, represented 5 out of 6 known cyber-physical attack frameworks.
- New variants of the Qbot infostealer were found. While earlier variants of Qbot were limited to password theft, newer variants include backdoor functionality and have been used in conjunction with REvil and other ransomware campaigns.

- Because known cyber-physical attacks are highly dependent upon command-and-control capabilities, limit unnecessary network connectivity and monitor for any unauthorized network communications.
- Due to the capabilities of cyber-physical attack frameworks – especially newer frameworks such as Industroyer, Industroyer 2 and Incontroller – it is increasingly important to protect infrastructure details about industrial control systems (ICS). Increased attention to the protection of system- and device-level configurations and settings is recommended.

CONCLUSION: ACTIVE USB CYBERSECURITY CONTROLS ARE INCREASINGLY IMPORTANT; MORE INCLUSIVE DOCUMENT MANAGEMENT AND CONTROL IS CRITICAL



For the sixth year in a row, the known threats attempting to enter industrial/OT environments have continued to increase in sophistication, frequency and potential risk to operations. USB-borne malware is clearly being leveraged as part of larger cyber attack campaigns against industrial targets. This indication is supported by the analysis of ATT&CK techniques, together with the presence of malware associated with major cyber-physical attack campaigns (e.g., Stuxnet, Black Energy, Triton, Industroyer and Industroyer 2).

It remains clear that modern malware variants have adapted to take advantage of the USB standards and are capable of leveraging USB removable media to circumvent network defenses and bypass the air gaps that many industrial facilities depend on for protection. Once successfully penetrated, techniques focus on information gathering, evading detection and enabling direct manipulation of target systems over the use of novel exploitations – all consistent with LotL tactics. Exploits that were seen focus heavily on document-based infections and misuse of internal scripting mechanisms. Continued diligence is necessary to defend against the growing USB threat, and strong USB security controls are highly recommended. In addition, an assessment of internal operations, with a focus on document handling and file sharing, is also recommended.

METHODOLOGY

By looking at a very specific vector into industrial automation environments, we obtain a unique opportunity to analyze the real malware threats that industrial organizations face. This is important because there are only a few real vectors in OT 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. Malicious USB devices and peripherals (e.g., BadUSB or other USB attack platforms), while increasingly popular and highly effective, are not included in this report.[8] This report focuses specifically on malware found on USB storage devices used to carry files into, out of and in between industrial facilities, as analyzed by Honeywell's Secure Media Exchange (SMX) product. The results are based on malware that has been successfully detected and blocked by SMX 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.

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 (RATs), although backdoors may also be specific to local systems or applications.

BADUSB

An exploitation of certain USB devices which allows the firmware to be overwritten by a hacker, modifying 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 provide 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 toward 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.

CYBER-PHYSICAL ATTACKS/FRAMEWORKS

Cyber-physical attacks refer to cyber attacks that are capable of creating a physical impact, typically by manipulating an industrial automation process to create physical destruction or some other hazardous condition. There are six known cyber-physical attack campaigns at the time of this report, each with corresponding malware frameworks that could facilitate further use of existing threats and/or further evolution of new threats. Read more in Honeywell's report "The Cyber-Physical Six: How Targeted Industrial Attacks Have Evolved and a Prediction of What's to Come."

GARD

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

INDUSTRIAL CONTROL SYSTEMS, ICS, INDUSTRIAL CONTROL, AUTOMATION SYSTEMS

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

"LIVING OFF THE LAND" A\ATTACK, LOTL

A "living off the land" attack refers to techniques used by attackers that do not directly engage in malicious activities. This type of attack is primarily focused on passive data gathering and information reconnaissance to better understand the target's infrastructure, vulnerabilities and potential entry points. In industrial systems, LotL techniques can also include the direct manipulation of process control and automation systems, using the system's inherent capabilities against itself.

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 full operational remediation and process recovery.

OPERATIONAL TECHNOLOGY, OT

Operational technology 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 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 TROJAN, 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, SMX

Secure Media Exchange is a commercial industrial cybersecurity technical solution developed by Honeywell and is designed to help users lower the risk of USB-borne threats. For more information, visit https://www.hwll.co/SMX.

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 any number of maliciously programmed USB devices. These are typically purpose-built devices designed to masquerade as other legitimate USB devices, but that possess any number of attack capabilities, including human interface device (HID) attacks, keylogging, data theft, remote access, and command and control.

USB-BORNE MALWARE

Any malware that is carried by or spread via a USB device. This typically refers to an infected file on a USB thumb drive or other storage device but could also refer to malware directly injected via a UAP.

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 connects via USB type-A interfaces using the USB standard "USBStor" device classification. However, the USB standard is diverse and other storage device types are available, while non-flash USBStor devices also exist.

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

Honeywell's Global Analysis, Research and Defense (GARD) team 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 Industrial 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.

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

White paper | Rev | 02/2024

THE FUTURE IS WHAT WE MAKE IT

Honeywell