2021 CYBER TRENDS AND INSIGHTS IN THE MARINE ENVIRONMENT

Coast Guard Cyber Command

United States Coast Guard

Approved for public release; distribution unlimited. Date: 5 August 2022

Disclosure: The information in this report is provided “as is” for informational purposes only. The U.S. Coast Guard does not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, by applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/.

If an entity wishes to create and distribute derivatives of this report they should: (1) provide notice to Coast Guard Cyber Command before distributing such derivatives and (2) refrain from affixing the Coast Guard Cyber logo or DHS seal to the derivatives, unless they have obtained written permission to do so from the Coast Guard Office of External Affairs.

The unauthorized use of any Federal agency’s seal is governed by the U.S. Code title 18 sections 506, 701, 709, and 1017. U.S. Code Title 14 section 934 prohibits individuals, corporations, and other businesses from using the words "Coast Guard" or "United States Coast Guard" for trade or business purposes.

Table of Contents

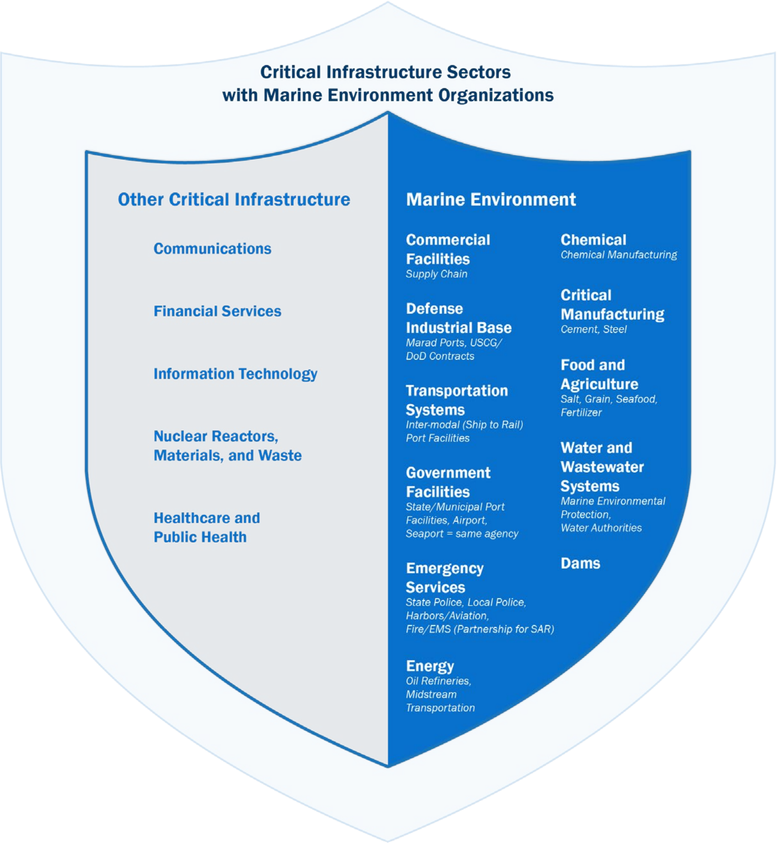
EXECUTIVE SUMMARY

Coast Guard in the Marine Environment

The U.S. Coast Guard has authority to prevent, detect, and respond to threats endangering Maritime Critical Infrastructure and Key Resources (CI/KR) entities. The Coast Guard is Co-Sector Risk Management Agency (SRMA) for the Transportation Sector and has responsibility for protecting maritime CI/KR. The Coast Guard shares this responsibility with the U.S. Department of Transportation and the Transportation Security Administration. U.S. Coast Guard Cyber Command (CGCYBER) is uniquely capable of conducting cyber operations to execute this mandate. In support of Coast Guard Sector Commanders, and CGCYBER will:

- Provide technical assistance to State, Local, Territorial, and Tribal (SLTT) entities by enhancing Maritime Critical Infrastructure cyber resilience within their Area of Responsibility (AOR).
- Participate in the Critical Incident Communication (CIC) process when necessary and support Maritime Security (MARSEC) Level change processes, as needed.
- Assist Federal and SLTT agency operations in the Marine Environment (ME).

This report aims to provide Coast Guard units and their port partners with relevant information to identify and address cyber risks. The Coast Guard recognizes the criticality of the ME and its inclusion in the wide range of other critical infrastructure sectors that operate within the marine environment, as illustrated below.

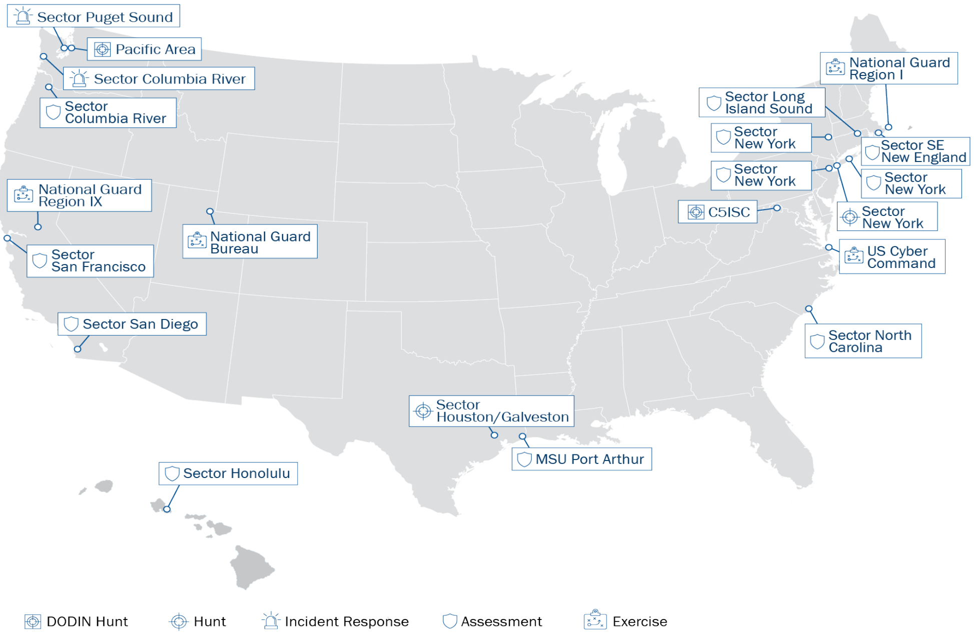

Critical Infrastructure Sectors
with Marine Environment Organizations
Other Critical Infrastructure
Communications
Financial Services
Information Technology
Nuclear Reactors, Materials, and Waste
Healthcare and Public Health
Marine Environment
Commercial Facilities
Supply Chain
Defense Industrial Base
Marad Ports, USCG/ DoD Contracts
Transportation Systems
Inter-modal (Ship to Rail) Port Facilities
Government Facilities
State/Municipal Port Facilities, Airport, Seaport = same agency
Emergency Services
State Police, Local Police, Harbors/Aviation, Fire/EMS (Partnership for SAR)
Energy
Oil Refineries, Midstream Transportation
Chemical
Chemical Manufacturing
Critical Manufacturing
Cement, Steel
Food and Agriculture
Salt, Grain, Seafood, Fertilizer
Water and Wastewater Systems
Marine Environmental Protection, Water Authorities
Dams

Cyber Protection Teams (CPTs)

CPTs are U.S. Coast Guard deployable specialized forces delivering Defensive Cyberspace Operations capability to prevent, detect, and respond to cyber threats to ME Critical Infrastructure. CPTs deliver capabilities to Coast Guard Operational Commanders and mission-partners through three core mission types:

1. Assessments: Providing threat emulation, vulnerability enumeration, and hardening recommendations.
2. Hunts: Proactively identifying adversary presence on networks and systems.
3. Incident Response: Consisting of interagency coordination, forensic support, and remediation guidance.

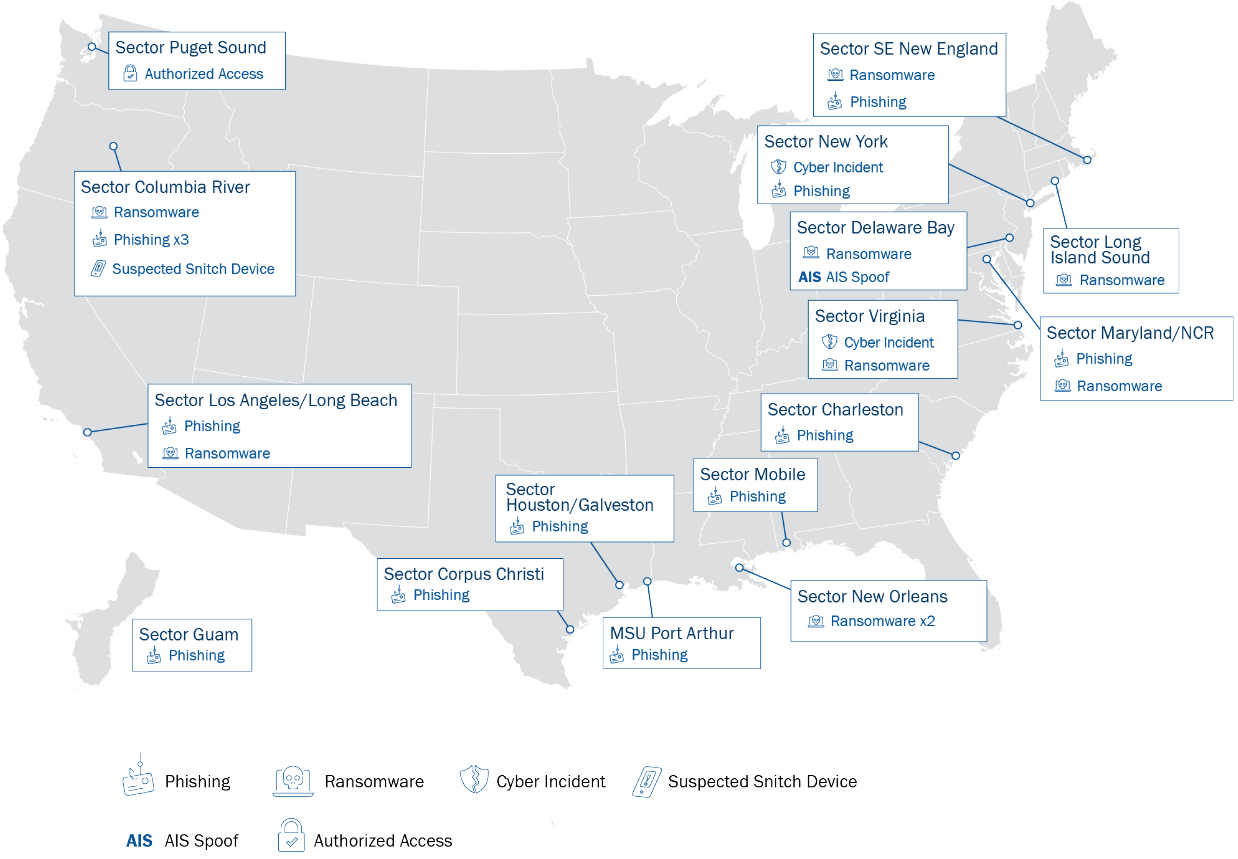
CGCYBER's first team, 1790 CPT, attained Full Operational Capability in May 2021. The second team, 2013 CPT, attained Initial Operating Capability in November 2021. CGCYBER CPTs have completed missions and exercises across the United States as shown below.



Maritime Cyber Readiness Branch (MCRB)

CGCYBER's MCRB is uniquely qualified, with expertise in marine safety and cybersecurity, to translate cybersecurity details into measurable operational risk. MCRB's risk analysis supports Coast Guard decision-makers and guides proper response actions. When a security incident is cybersecurity-related, the MCRB plays a crucial role in helping operational field units assess risk.

In 2021, MCRB investigated 47 cybersecurity incidents, including several large-scale incidents affecting multiple organizations at once. Though the number of reported incidents has increased 68% from 2020 (28 total incidents) and 176% since 2019 (17 total incidents), MCRB believes many other incidents go undetected or unreported. MCRB investigates all security incidents in the Marine Transportation System (MTS) for evidence of a Breach of Security (BoS) and/or Transportation Security Incident (TSI). The Coast Guard's primary concerns are risks to the safety and security of the port and impacts in the MTS. The map below illustrates all ME-related cyber incidents reported to the Coast Guard in 2021.



Introduction to Trends and Insights: 2021

This report aims to continue the Coast Guard's tradition of collaborating with owners and operators in the ME to provide relevant information about best practices to secure their critical systems based on Coast Guard findings. This report intends to aid Sector Commanders, their staffs, and maritime facility leadership teams, including Facility Security Officers (FSOs), IT Directors, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and other executives. It supports their ability to identify and address cyber risks within their purview. This report contains a detailed summary of findings along with mitigations applicable to a variety of owners and operators. Below are some of the key takeaways:

Access Control & Authentication

- Easily Guessable Credentials
- Weak Password Policy
- Easily Crackable Passwords
- *May relate to Security Measures for Access Control (i.e., 33 CFR 105.255)*

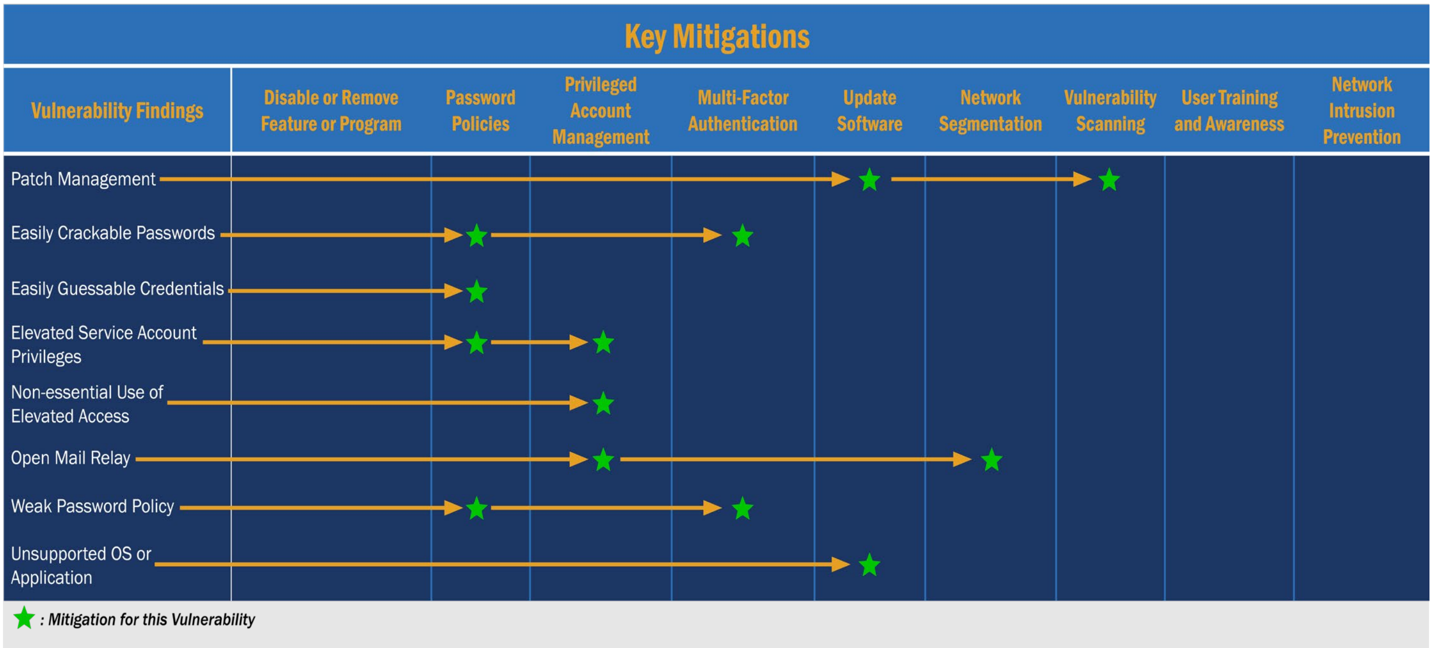
Least Privilege

- Elevated Service Account Privileges
- Non-essential Use of Elevated Access
- Open Mail Relay
- *May relate to Security Measures for Restricted Areas (i.e., 33 CFR 105.260)*

System Maintenance

- Patch Management
- Unsupported OS
- *May relate to Security Systems and Equipment Maintenance (i.e., 33 CFR 105.250)*

Each of the above findings ties to specific Common Mitigation Recommendations shown in the below graphic. The report describes each recommendation in detail within the section titled “Common Mitigation Recommendations”.



Key Mitigations

Vulnerability Findings	Disable or Remove Feature or Program	Password Policies	Privileged Account Management	Multi-Factor Authentication	Update Software	Network Segmentation	Vulnerability Scanning	User Training and Awareness	Network Intrusion Prevention
Patch Management					★		★		
Easily Crackable Passwords		★		★					
Easily Guessable Credentials		★							
Elevated Service Account Privileges		★	★						
Non-essential Use of Elevated Access			★						
Open Mail Relay			★			★			
Weak Password Policy		★		★					
Unsupported OS or Application					★				

★ *: Mitigation for this Vulnerability*

BACKGROUND

Cyber Threats to the Marine Environment

Cyber incidents pose a significant threat to the MTS. The graphic below illustrates six key cyber threats to a port facility.

Port Components at Risk

1 Facility Access
A compromise impacting physical access control systems can lead to supply chain delays and localized traffic congestion in the vicinity of a port.

2 Terminal Headquarters – Data
Terminal and Gate Operating Systems (TOS/GOS) streamline the flow of cargo in a port. A compromise of a port's TOS/GOS data could result in leaks of sensitive supply chain data from port customers. Manipulation of TOS/GOS data could also be used for smuggling or cargo theft.

3 Terminal Headquarters – Ransomware
A ransomware attack affecting TOS/GOS systems could make critical systems and data inaccessible. This could lead to a full stop of port operations, resulting in financial losses and supply chain disruptions.

4 Operational Technology (OT) Systems
Maritime infrastructure relies on various OT systems to control pumps, cranes, and other industrial equipment. The compromise of an OT system can cause safety issues and lead to loss of life or property. In addition, a compromise can disrupt facility operations.

5 Positioning, Navigation, and Timing (PNT)
PNT often supports many vessels within a port's vicinity, and is critical to maritime operations. Loss of PNT can impede vessels' ability to safely navigate a port, and lead to an increased risk of collisions and groundings. Any of these events can result in environment damage, loss of life or property, or a disruption to safe navigation.

6 Vessel
A compromise to shipboard systems could impact a vessel's ability to safely navigate and manage their cargo. A vessel compromise could also lead to disruption of shore-side systems, because lateral movement is possible through shared wireless or wired networks, portable media, and other interconnections.

Criminal's Use of Ransomware

During calendar year 2021 (CY21), cyber criminals continued to target MTS entities by exploiting traditional ransomware and Ransomware as a Service (RaaS). Cyber-criminals are now using more advanced tactics, techniques, and procedures (TTPs) including focused ransomware attacks in multi-extortion style campaigns with hopes of ensuring a higher, more guaranteed payout. Rather than hitting a broad range of targets, cyber criminals have evolved to focus ransomware attacks on higher value targets. The three most popular RaaS variants used to target the MTS in this period were Maze, Sodinokibi, and Ryuk. According to publicly available information, these three RaaS families are consistently among the top five variants used across all industries in 2020 and 2021.

Nation States Improving Tactics

Nation state malicious cyber actors (MCAs) typically abuse zero-day vulnerabilities and known exploitations. Zero-day vulnerabilities are vulnerabilities disclosed or discovered without an available patch or update to remediate the vulnerability. MCAs often use zero-day vulnerabilities in their initial attack vector to avoid detection. Nation state MCAs abuse Virtual Private Servers (VPS) and web shells to avoid detection and circumvent host system security in order to gain access to the victim networks. MCAs use these techniques within the MTS to increase the probability of successfully exploiting an intended victim.

Phishing Attacks

In 2021, phishing remained the most prevalent means by which MCAs delivered malicious code. Cyber-criminals and nation state MCAs will very likely continue to use phishing emails to gain initial access to victim networks. There was an overall increase in phishing reporting in 2021, mirroring trends in phishing activities observed globally by the Anti-Phishing Working Group (APWG).[1] In 2021, industries within the ME, like logistics and shipping, have seen slight increases in activity.

Looking Forward

The significance of cybersecurity in the MTS grew exponentially in 2021, driven by two major factors: 1) A 68% increase in the number of reported MTS cyber incidents and 2) the Coast Guard's steps to ensure that Maritime Transportation Security Act (MTSA) regulated facilities are complying with guidance issued in Navigation and Vessel inspection Circular (NVIC) 01-20, Guidelines for Addressing Cyber Risks at MTSA-Regulated Facilities.

As of October 1, 2021, MTSA-regulated facilities are required to address cybersecurity risks and vulnerabilities in their facility security plans and facility security assessments. This policy brought with it new cyber competency expectations for industry facility security officers and Coast Guard facility inspectors. Coast Guard facility inspectors will review cybersecurity plans submitted by facilities. They will also incorporate cybersecurity reviews when conducting security inspections.

The MCRB is the bridge between the U.S. Coast Guard's traditional Marine Safety mission and the cybersecurity domain. They are uniquely qualified for this role, with a workforce combining decades of marine safety experience with cybersecurity training and expertise. The MCRB utilizes this expertise to support both Coast Guard field units and the broader MTS in a variety of ways such as:

- Cyber threat/vulnerability information sharing products such as Maritime Cyber Alerts
- Training for field units on the Coast Guard's role regarding MTS cybersecurity
- Support to field units investigating MTS cyber incidents

[1] Source: https://apwg.org/trendsreports

FINDINGS AND INSIGHTS: METHODOLOGY

Assess Mission

CGCYBER CPTs conduct Assess missions using the Cybersecurity Infrastructure Security Agency's (CISA) Risk and Vulnerability Assessments (RVAs) process. The RVA process is used to assess an organization's overall effectiveness in identifying and addressing network vulnerabilities. For the 10 CY21 missions, CGCYBER provided results using language that aligns with CISA and industry standards applied in the MITRE ATT&CK®[2] framework.

The MITRE ATT&CK®[3] framework aims to build a community-driven knowledge repository based on known TTPs employed by threat actors. This framework helps develop threat models and facilitate vulnerability mitigation efforts. It includes 14 distinct attack paths that cyber adversaries use to obtain and maintain unauthorized access to a network/system.

CGCYBER mapped each result and attack path step to the appropriate MITRE ATT&CK tactic and compiled detailed mitigation actions from the data to show the most common mitigations identified during CPT missions.

Hunt Mission

CGCYBER CPTs conduct Hunt missions use best practices aligned with CISA's Hunt and Incident Response Team (HIRT). CGCYBER CPTs identify indicators of compromise using industry-standard network and endpoint detection tools as well as commercial threat intelligence tools. The CPTs conducted four Hunt missions during CY21 on commercial and government owned networks critical to the MTS. Relevant findings from missions are anonymized, shared with stakeholders, and provide essential context for this report. Appendix B, C, and D show some publicly released notifications from the CPT's Hunt missions.

Incident Response

CGCYBER CPTs work closely with the MCRB to respond to incidents reported to the Coast Guard. Teams offer technical assistance to Coast Guard field commanders and affected entities in their area of responsibility (AOR). The CPTs responded to five incidents in CY21, providing technical analysis. CGCYBER CPTs closely coordinate with CISA, the Federal Bureau of Investigation (FBI) and other federal, state, and local law enforcement partners to report and distribute adversary TTPs and detailed indicators of compromise to the broader community. The CPTs also provide tailored remediation recommendations to affected entities and Coast Guard Captains of the Port (COTP).

[2] "© 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation."

[3] Source: https://us-cert.cisa.gov/best-practices-mitre-attckr-mapping

SUMMARY OF FINDINGS

As shown below, MTS partners fully remediated two-thirds (⅔) of all exploitable findings on publicly facing systems and 45% of all internally exploitable findings within six months of a CPT Assess mission. They also partially remediated an additional one-sixth (⅙) of publicly facing and 43% of internally accessible findings within this 6-month window.

Mitigation Status based on 6-Month Follow-Up with Entity

Publically Exploitable Findings

14 ☑ Fully mitigated

2 Accepted risk of finding
3 False positive
3 No action to date

Internally Exploitable Findings

53 ☑ Fully mitigated

46 Partially mitigated
5 Accepted risk of finding
0 False positive
8 No action to date

Social Engineering Findings

7 ☑ Fully mitigated

5 Partially mitigated
0 Accepted risk of finding
4 No action to date

The below table shows the individual findings from the 10 Assess missions conducted from December 2020 to December 2021. This table categorizes our results into Publicly Exploitable findings, Internally Exploitable findings, and Social Engineering findings.

Summarized Findings from 2021 CPT Assess Missions

Finding	Internally Exploitable	Publicly Exploitable	Publicly Exploitable & Internally Exploitable	Social Engineering
Insecure Default Configuration	10	0	0	0
Data Disclosure	4	4	0	0
Spear Phishing Weaknesses	0	0	0	9
Patch Management	7	1	0	0
Spear Phishing Susceptibility	0	0	0	8
Easily Crackable Passwords	7	0	0	0
Easily Guessable Credentials	5	2	0	0
Unnecessary Network Services	6	1	0	0
Account Privileges	5	1	0	0
Clear-text Password Disclosure	6	1	0	0
Elevated Service Account Privileges	6	0	0	0
Exposed Administrative Interface	2	4	0	0

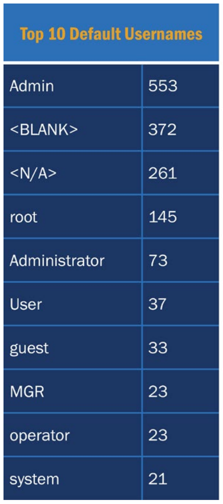
Finding	Internally Exploitable	Publicly Exploitable	Publicly Exploitable & Internally Exploitable	Social Engineering
Non-essential Use of Elevated Access	6	0	0	0
Open Mail Relay	6	0	0	0
Weak Password Policy	6	0	0	0
Unsupported OS or Application	5	0	0	0
Clear-text Protocols	3	0	0	0
Insecure Web Service	3	1	0	0
Admin Password Reuse	3	0	0	0
Insecure File Shares	3	0	0	0
Insecure Password Storage	2	0	0	0
Network Segregation Not Implemented	3	0	0	0
PII Disclosure	3	0	0	0
Username Enumeration	1	2	0	0
Authentication Bypass	1	0	0	0
Insecure Database Configuration	1	0	0	0
Default Printer Credentials	2	0	0	0
Directory Traversal	0	1	0	0
Easily Accessible OT Systems	1	0	0	0
Elevated Password Reuse	2	0	0	0
Industrial Control System Architecture	1	0	0	0
Insecure Logon Configuration	2	0	0	0
Insecure Service Permissions	1	1	0	0
Navigation System Updates	1	0	0	0
Port Security	1	0	0	0
Possible Previous Compromise	0	1	0	0
Self-Signed Certificates	0	1	0	0
Sensitive Data Exfiltration	1	0	0	0
Session Management	1	0	0	0
Similar Public Domains	0	1	0	0

Finding	Internally Exploitable	Publicly Exploitable	Publicly Exploitable & Internally Exploitable	Social Engineering
Unnecessary Default Feature Enabled	1	0	0	0
Weak Authentication Mechanism	1	0	0	0
Web Service Directory Traversal	0	1	0	0
Web Application Vulnerability	1	0	0	0

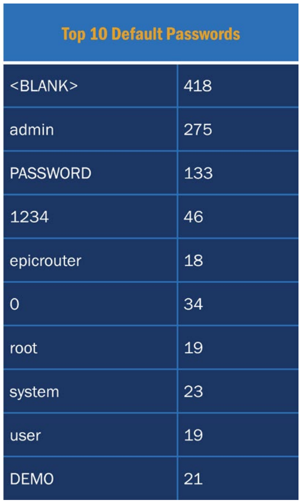
COMMON FINDINGS

Easily Guessable Credentials

One or more services are accessible using an easily guessed username and password. An attacker with minimal technical knowledge can use these credentials to access the related services. The below tables show some of the most common default usernames and passwords, along with the number of unique technology vendors that utilize them. The information comes from a public analysis of 2,866 vendor products[4].



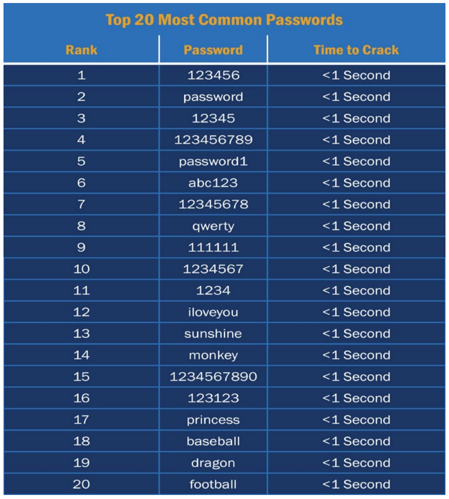
Top 10 Default Usernames	
Admin	553
<BLANK>	372
<N/A>	261
root	145
Administrator	73
User	37
guest	33
MGR	23
operator	23
system	21



Top 10 Default Passwords	
<BLANK>	418
admin	275
PASSWORD	133
1234	46
epicrouter	18
0	34
root	19
system	23
user	19
DEMO	21

Easily Crackable Passwords

User account passwords on the system are common and widely used. An attacker can successfully predict the victim's password, using a wordlist to gain access to the account. The below table shows the twenty most common passwords used according to several data breach repositories from NordPass.[5] Using a common password can greatly increase the probability of an attacker accessing an account without authorization.



Top 20 Most Common Passwords

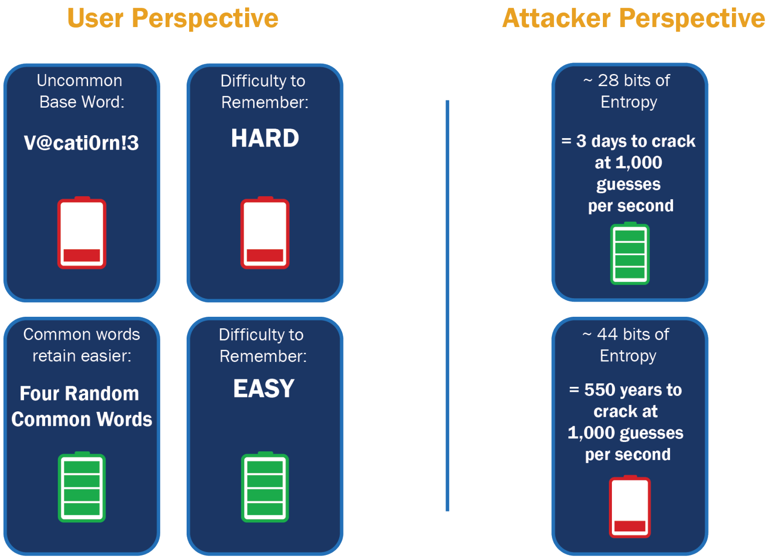
Rank	Password	Time to Crack
1	123456	<1 Second
2	password	<1 Second
3	12345	<1 Second
4	123456789	<1 Second
5	password1	<1 Second
6	abc123	<1 Second
7	12345678	<1 Second
8	qwerty	<1 Second
9	111111	<1 Second
10	1234567	<1 Second
11	1234	<1 Second
12	iloveyou	<1 Second
13	sunshine	<1 Second
14	monkey	<1 Second
15	1234567890	<1 Second
16	123123	<1 Second
17	princess	<1 Second
18	baseball	<1 Second
19	dragon	<1 Second
20	football	<1 Second

[4] Source: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv

[5] Source: https://nordpass.com/most-common-passwords-list/

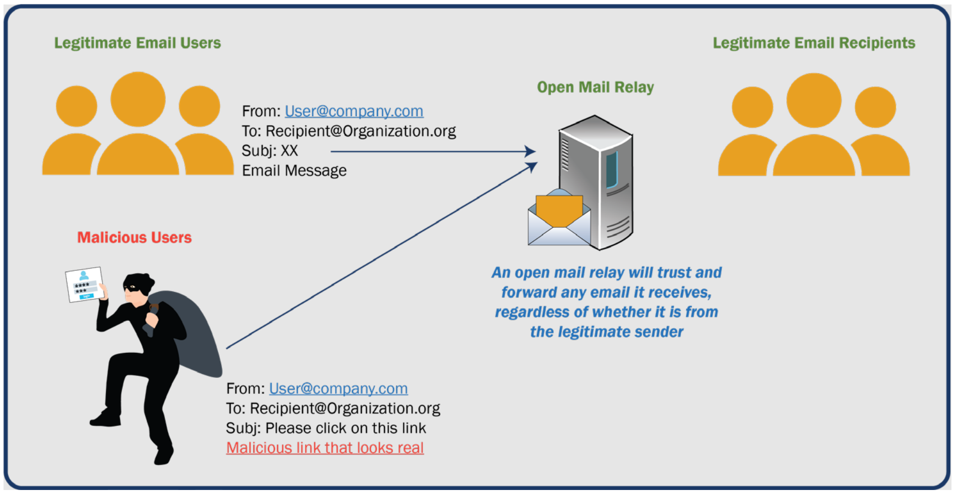
Weak Password Policy

A weak password policy can result in an attacker gaining unauthorized access to a system or application. According to the National Institute of Standards and Technology (NIST), a strong password includes password length, complexity, minimum password age, and history. It also contains suggestions for enforcement and consequences when not followed (lost system access). A good password policy can protect an organization from brute force password cracking, guessing, and reuse. The below graphic displays a method of forming secure passwords that are still user-friendly. The image borrows from analysis published by Randall Munroe on xkcd.com.[6]



Open Mail Relay

An open mail relay is an email server that allows anonymous users to send emails. There is no authentication when using an open mail relay. Open mail relays will send emails with spoofed source addresses that appear to be coming from legitimate addresses within your organization. MCAs often use open mail relays to send phishing emails and spam.



From: User@company.com
To: Recipient@Organization.org
Subj: XX
Email Message

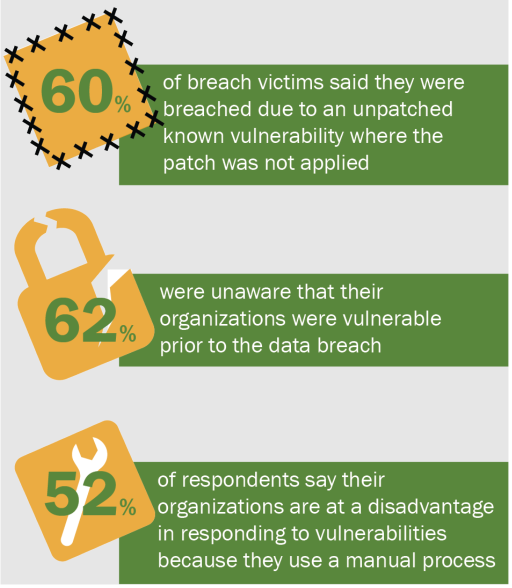
An open mail relay will trust and forward any email it receives, regardless of whether it is from the legitimate sender

From: User@company.com
To: Recipient@Organization.org
Subj: Please click on this link
Malicious link that looks real

[6] Source: https://xkcd.com/936/

Patch Management

Vendors release patches and updates to address existing and emerging security threats and address multiple levels of criticality. Failure to apply the latest patches can leave the system open to attack with publicly available exploits. The risk presented by missing patches and updates can vary. The graphic below was created using information from ServiceNow.[7]



60% of breach victims said they were breached due to an unpatched known vulnerability where the patch was not applied

62% were unaware that their organizations were vulnerable prior to the data breach

52% of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use a manual process

Unsupported OS or Application

Vendors do not patch unsupported software or hardware, creating a significant security risk. There is no way to address security vulnerabilities on these devices to ensure that they are secure. The overall security posture of the entire network is at risk because an attacker can target these devices to establish an initial foothold into the network. The graphic below was created using information from a Private Industry Notification put out by the FBI.[8]

SYSTEM ERROR

Windows 7 Operating System has 680 known exploits since Microsoft stopped providing updates in 2020

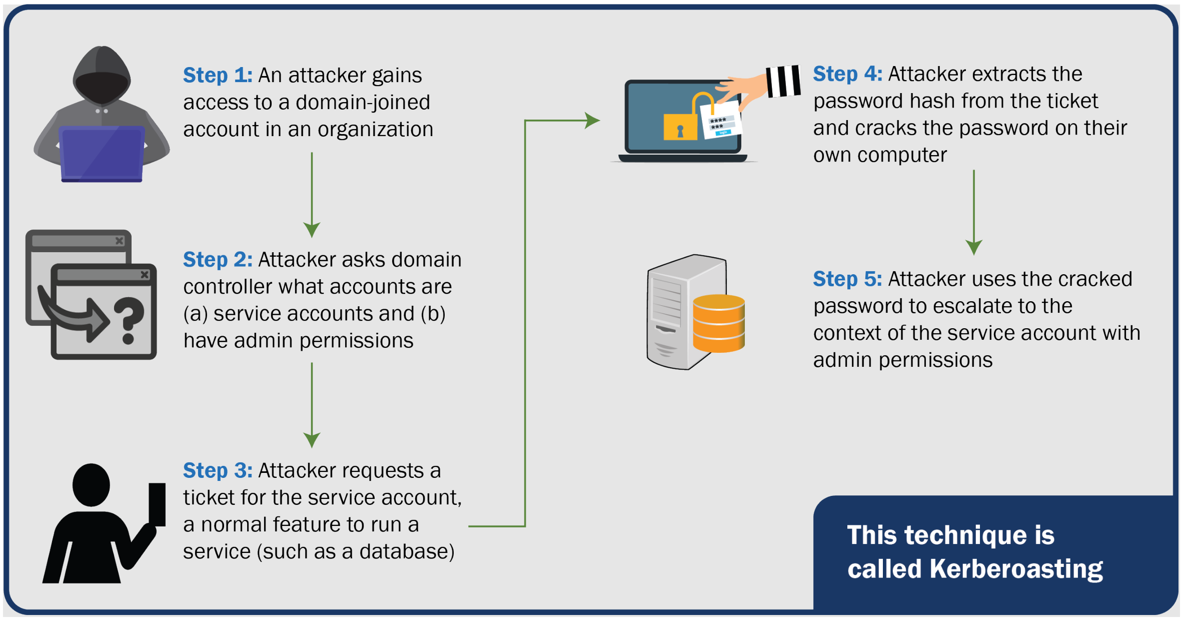
98% of systems infected with WannaCry ran Windows 7 unsupported

[7] Source: https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

[8] Source: https://www.documentcloud.org/documents/7013545-Windows-7-End-of-Life-PIN-20200803-002-BC.html

Elevated Service Account Privileges

Applications often require user accounts to operate, known as Service Accounts. Service Accounts use elevated privileges to perform a business function. MCAs leverage techniques, such as AS-REP roasting and Kerberoasting, to abuse legitimate functionality to attain a copy of the Service Account's password hash. If the service account has a weak password, the MCA can crack this password and access systems in the context of the Service Account. For simplicity, administrators often use existing administrator accounts as Service Accounts or create a new account and add the new Service Account to an existing administrator group, such as, Domain Administrators. MCAs often leverage these unnecessary permissions to gain full control over an enterprise.



Step 1: An attacker gains access to a domain-joined account in an organization

Step 2: Attacker asks domain controller what accounts are (a) service accounts and (b) have admin permissions

Step 3: Attacker requests a ticket for the service account, a normal feature to run a service (such as a database)

Step 4: Attacker extracts the password hash from the ticket and cracks the password on their own computer

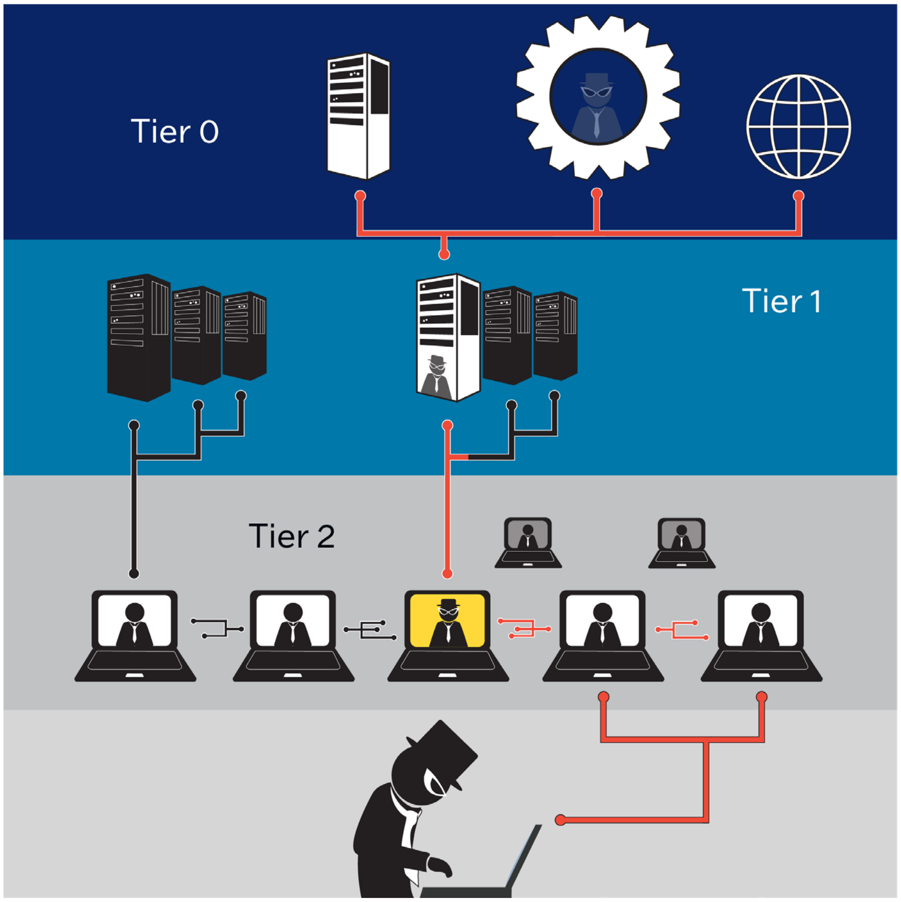
Step 5: Attacker uses the cracked password to escalate to the context of the service account with admin permissions

This technique is called Kerberoasting

Non-Essential Use of Elevated Access

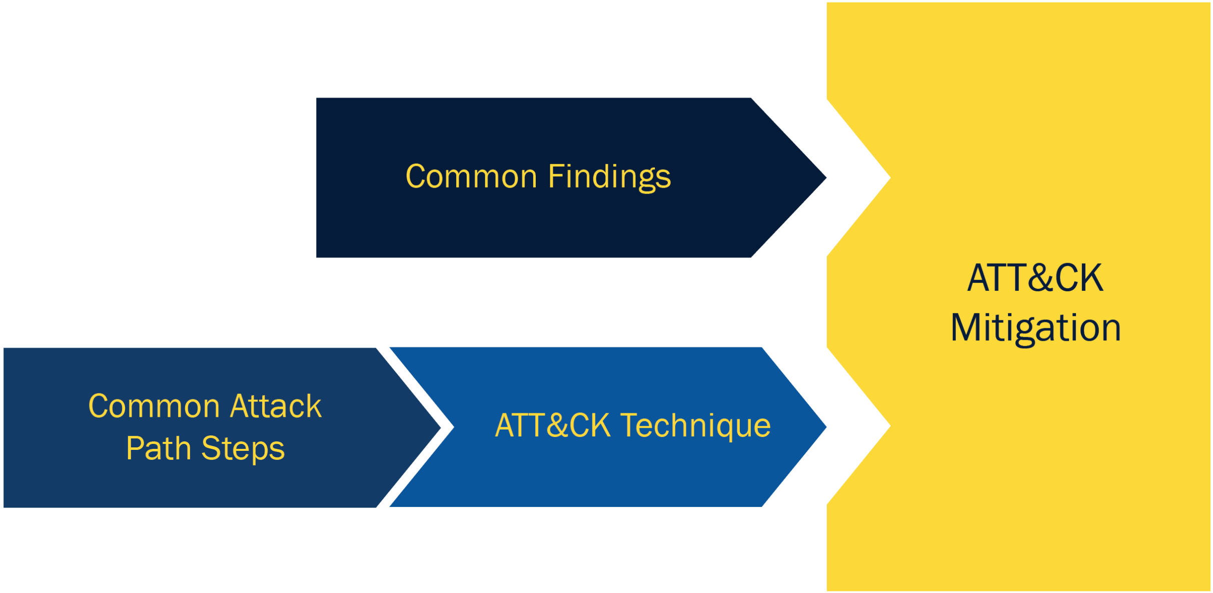
IT personnel use domain administrator accounts for system and network management because these typically have broad access permissions. Many organizations do not require separate accounts for normal business functions, such as email and web browsing, and their computer administrator tasks. An MCA who compromises an administrator account has significantly more access then if they were to compromise a standard user. An MCA with access to an administrator account on a compromised host can steal the account's authentication token generated by Active Directory and use it to operate using the elevated permissions. Using an elevated account throughout the domain for normal day-to-day tasks increases this risk.

The below image shows the privilege escalation path by an MCA through an enterprise. If an attacker can gain access to a workstation administrator (Tier 2) account on a device normally used to access email or the web, they will be able to access all credentials stored on this device. If server administrator (Tier 1) or domain/enterprise administrator (Tier 0) accounts are used on workstations accessible by this Tier 2 administrator, the MCA can access the Tier 1 or Tier 0 credentials from these devices and use them to access critical information or assert full control over the enterprise.



COMMON MITIGATION RECOMMENDATIONS

In addition to the common findings, we have included the attack paths from each mission in Appendix A to show the specific attack path steps tied to the appropriate corresponding ATT&CK technique. These attack paths demonstrate the steps taken by an MCA to gain initial access, move through a network, and deliver cyber effects. CGCYBER CPTs apply real-world MCA techniques to show how vulnerabilities can be exploited, and what the business impact would be. See Appendix A for a complete summary.



CGCYBER tabulated a complete list of all reported common findings and common attack path steps to drive recommended mitigation actions. For Common Findings, our team mapped each finding directly to one or more ATT&CK mitigation recommendations. For the attack path steps, each step maps to an ATT&CK technique and one or more ATT&CK mitigation recommendations. CGCYBER determined eighteen successful attack paths from threat emulation or detection during a Hunt mission. Appendix A contains detailed Attack Path data. The below table summarizes this data.

Mitigation Recommendation	Mapped Findings	Mapped Techniques
Password Policies	44 (1st)	35 (1st)
Privileged Account Management	31 (2nd)	23 (2nd)
Network Segmentation	23 (3rd)	13 (5th)
Multi-factor Authentication	22 (4th)	18 (3rd)
Vulnerability Scanning	20 (5th)	7 (7th)
Update Software	19 (6th)	4
User Training	15 (7th)	15 (4th)
Disable or Remove Feature or Program	8	11 (6th)

Summary of Effort & Resources Required for Mitigation Recommendations

	User Resistance	Upfront Cost	Recurring Cost
Disable or Remove Feature or Program	🟡	$ $ $	$
Password Policies	🔴	$	$
Multi-factor Authentication	🟡	$ $ $	$ $
Privileged Account Management	🟡	$ $ $	$ $
Network Intrusion Prevention	🟢	$ $ $	$ $
Network Segmentation	🟢	$ $ $	$ $
Vulnerability Scanning	🟢	$ $ $	$ $
Update Software	🟢	$ $ $	$ $
Logging	🟢	$ $ $	$ $ $

Common Mitigation #1: Disable or Remove Feature or Program

Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

STOPGAP Measure 1

Change default application for script file extensions such as .hta, .js, .vbs, .vbe, .wsf and .ps1 to Notepad.[3]

STOPGAP Measure 2

Use application control or filesystem permissions to block execution from user profile directories, including %AppData%, %LocalAppData%, their subdirectories, as well as %TEMP%.

Disable Commonly Exploited Features

Office Features	Web App Features	Remote Access	Administrative Features	Scripts	Deprecated Windows Features
Macros	php eval()	SSH	Unnecessary shells	.hta	LL-MNR
ActiveX Content		VNC	Powershell	.js	NetBIOS
Disable DDE execution in Word and Excel		RDP	WinRM	.jse	mshta.exe
Disable automatic DDE/OLE execution			InstallUtil	.vbs	cmstp.exe
			MMC	.vbe	Odbcconf.exe
			mavinject.exe	.wsf	Autorun for removable media
			Regsvcs	.ps1	Do not allow storage of passwords and credentials for network authentication
			Regasm		
			vercisid.exe		
			AlwaysInstallEvevated		
			InstallUtil.exe		
			mshta.exe		
			MSBuild		

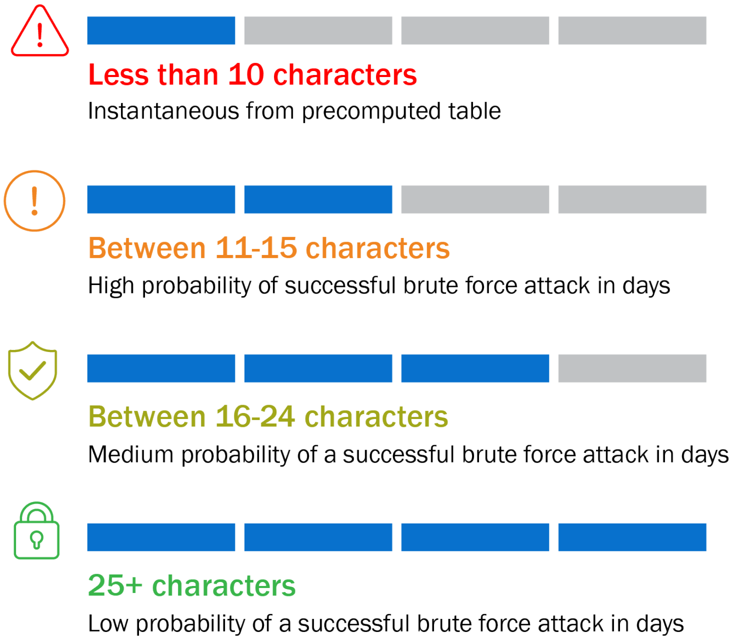
What does the Coast Guard do?

- The Coast Guard, along with the Department of Defense utilizes a Secure Host Baseline. The Windows baseline is available at: https://github.com/nsacyber/Windows-Secure-Host-Baseline
- The Department of Defense also releases several Security Technical Implementation Guides (STIGs). These guides provide implementation instructions for many features and applications. Most are publicly available at: https://public.cyber.mil/stigs/
- Many vendors also provide scripted solutions to implement STIGs for their products in public repositories.

Common Mitigation #2: Password Policies

Set and enforce secure password policies for accounts. Despite widespread frustration with the use of passwords from both a usability and security standpoint, they remain a very widely used form of authentication. Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose easily guessed passwords. One effective technique is to use pass phrases; using multiple words can add significant length to a password but still require significant mathematical computation to crack. Password managers offer greater security and convenience for the use of passwords to access online services. Greater security is achieved principally through the capability of most password manager applications to generate unique, long, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords either through a local or cloud-based vault.[9]

Length	**Password length is the primary factor in characterizing password strength.** Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.
Complexity	Composition rules increase the difficulty of guessing user-chosen passwords. Research has shown, however, that users respond in very predictable ways to the requirements imposed by composition rules.
Randomly-Chosen Secrets	Randomly-Chosen Secrets that are uniformly distributed will be more difficult to guess or brute-force attack than user-chosen secrets meeting the same length and complexity requirements.



Less than 10 characters

Instantaneous from precomputed table

Between 11-15 characters

High probability of successful brute force attack in days

Between 16-24 characters

Medium probability of a successful brute force attack in days

25+ characters

Low probability of a successful brute force attack in days

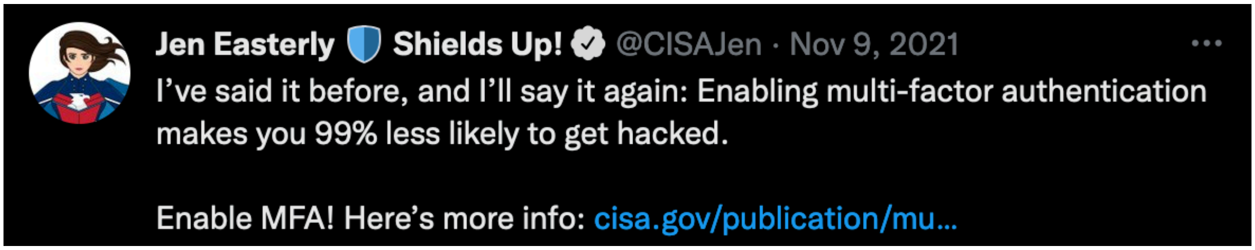
[9] Source: NIST Special Publication 800-63 Digital Identity Guidelines, available at: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.

Common Mitigation #3: Multi-Factor Authentication

Use two or more means to authenticate to a system, such as a username and a password in addition to a token from a physical smart card or token generator.

Something you know | Something you have | Something you are

CISA Director Jen Easterly promoted Multi-Factor Authentication(MFA) on Twitter:



Jen Easterly 🛡 Shields Up! ✓ @CISAJen · Nov 9, 2021

I've said it before, and I'll say it again: Enabling multi-factor authentication makes you 99% less likely to get hacked.

Enable MFA! Here's more info: cisa.gov/publication/mu…

Authentication Mechanisms[10]

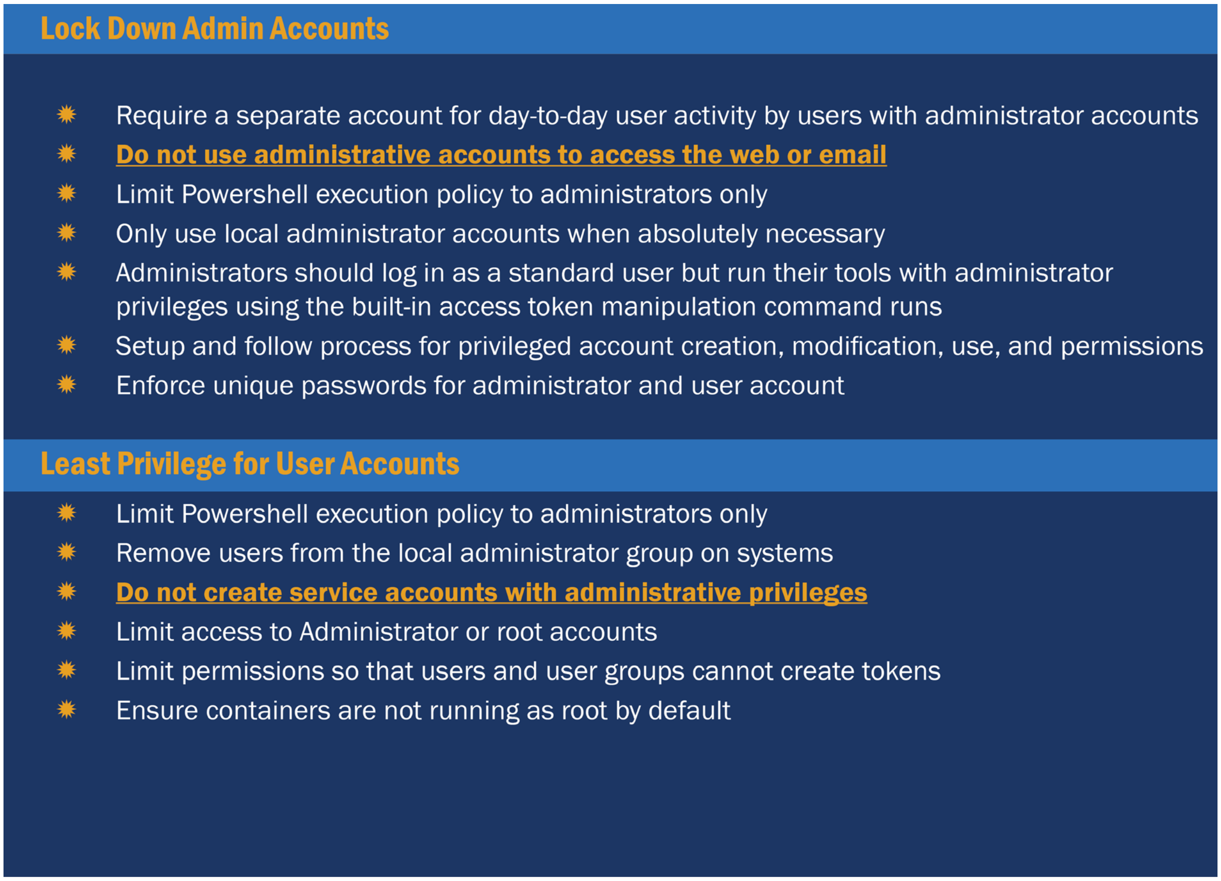
Memorized Secrets 	A Memorized Secret authenticator — commonly referred to as a **password** or, if numeric, a **PIN** — is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorized secret is *something you know.*
Look-Up Secrets 	A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the claimant and the credential service provider (CSP). The claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier. For example, the verifier may ask a claimant to provide a specific subset of the numeric or character strings printed on a card in table format. A common application of look-up secrets is the use of "recovery keys" stored by the subscriber for use in the event another authenticator is lost or malfunctions. A look-up secret is *something you have*.

[10] Sources:
- NIST Special Publication 800-63B, available at: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.
- CISA Multi-Factor Authentication Fact Sheet, available at: https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf

Out-of-Band Devices 	An out-of-band authenticator is a physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel. The claimant possesses and controls the device and supports private communication over this secondary channel, separate from the primary channel for e-authentication. An out-of-band authenticator is *something you have*.
Single-Factor One Time Password (OTP) Device 	A single-factor OTP device generates OTPs. This category includes hardware devices and software-based OTP generators installed on devices such as mobile phones. These devices have an embedded secret used as the seed for generation of OTPs and does not require activation through a second factor. The device displays the OTP and manually input for transmission to the verifier, thereby proving possession and control of the device. For example, an OTP device may display 6 characters at a time. A single-factor OTP device is *something you have*.
Multi-Factor OTP Devices 	A multi-factor OTP device generates OTPs for use in authentication after activation through an additional authentication factor. This includes hardware devices and software-based OTP generators installed on devices such as mobile phones. The second factor of authentication may be achieved through integral entry pad, an integral biometric (e.g., fingerprint) reader, or a direct computer interface (e.g., USB port). The device displays the OTP for manual input for transmission to the verifier. For example, an OTP device may display 6 characters at a time, thereby proving possession and control of the device. The multi-factor OTP device is *something you have* activated by either *something you know* or *something you are*.
Single-Factor Cryptographic Software 	A single-factor software cryptographic authenticator is a cryptographic key stored on a disk or some other "soft" media. Possession and control of the key allows for authentication. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The single-factor software cryptographic authenticator is *something you have*.
Single-Factor Cryptographic Devices 	A single-factor cryptographic device is a hardware device that performs cryptographic operations using protected cryptographic key(s) and provides the authenticator output via direct connection to the user endpoint. The device uses embedded symmetric or asymmetric cryptographic keys and does not require activation through a second factor of authentication. Possession of the device via the authentication protocol allows for authentication. The authenticator output provides direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. A single-factor cryptographic device is *something you have*.

Multi-Factor Cryptographic Software	A multi-factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media that requires activation through a second factor of authentication. Possession and control of the key allows for authentication. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The multi-factor software cryptographic authenticator is *something you have* activated by either *something you know* or *something you are*.
Multi-Factor Cryptographic Devices	A multi-factor cryptographic device is a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor. Possession and control of the key allows for authentication. The authenticator output provides direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. The multi-factor cryptographic device is *something you have* activated by either *something you know* or *something you are*.

Common Mitigation #4: Privileged Account Management



Lock Down Admin Accounts

- Require a separate account for day-to-day user activity by users with administrator accounts
- **Do not use administrative accounts to access the web or email**
- Limit Powershell execution policy to administrators only
- Only use local administrator accounts when absolutely necessary
- Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command runs
- Setup and follow process for privileged account creation, modification, use, and permissions
- Enforce unique passwords for administrator and user account

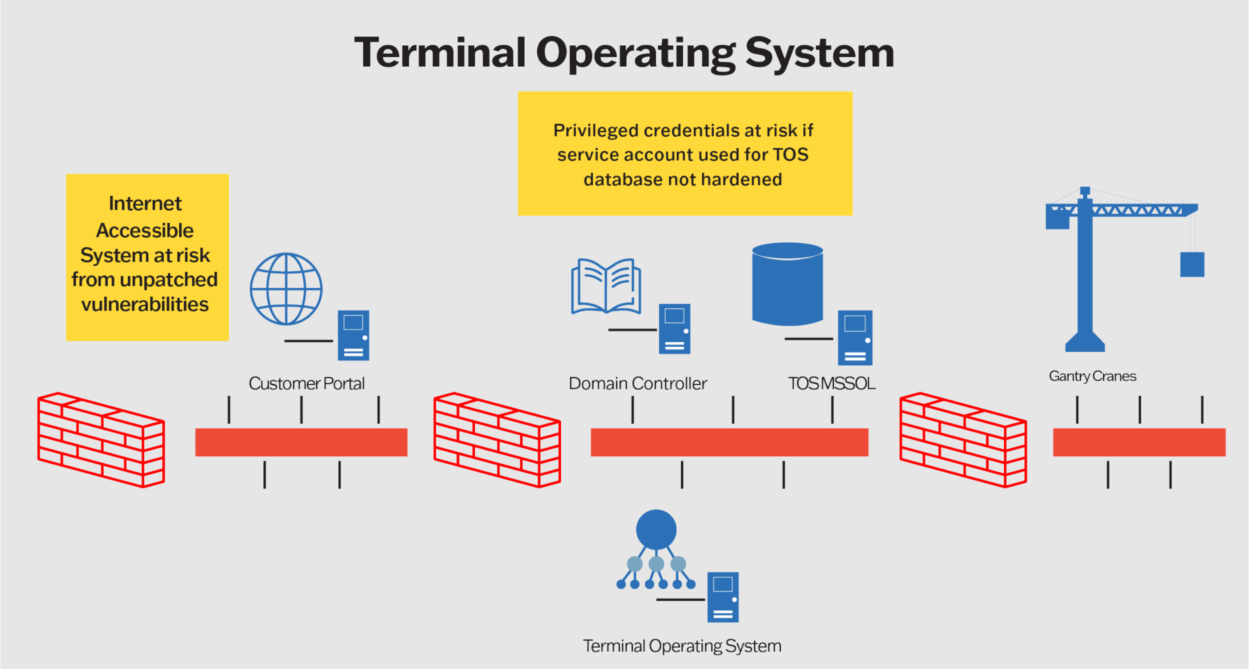
Least Privilege for User Accounts

- Limit Powershell execution policy to administrators only
- Remove users from the local administrator group on systems
- **Do not create service accounts with administrative privileges**
- Limit access to Administrator or root accounts
- Limit permissions so that users and user groups cannot create tokens
- Ensure containers are not running as root by default

Spotlight on Terminal Operating Systems

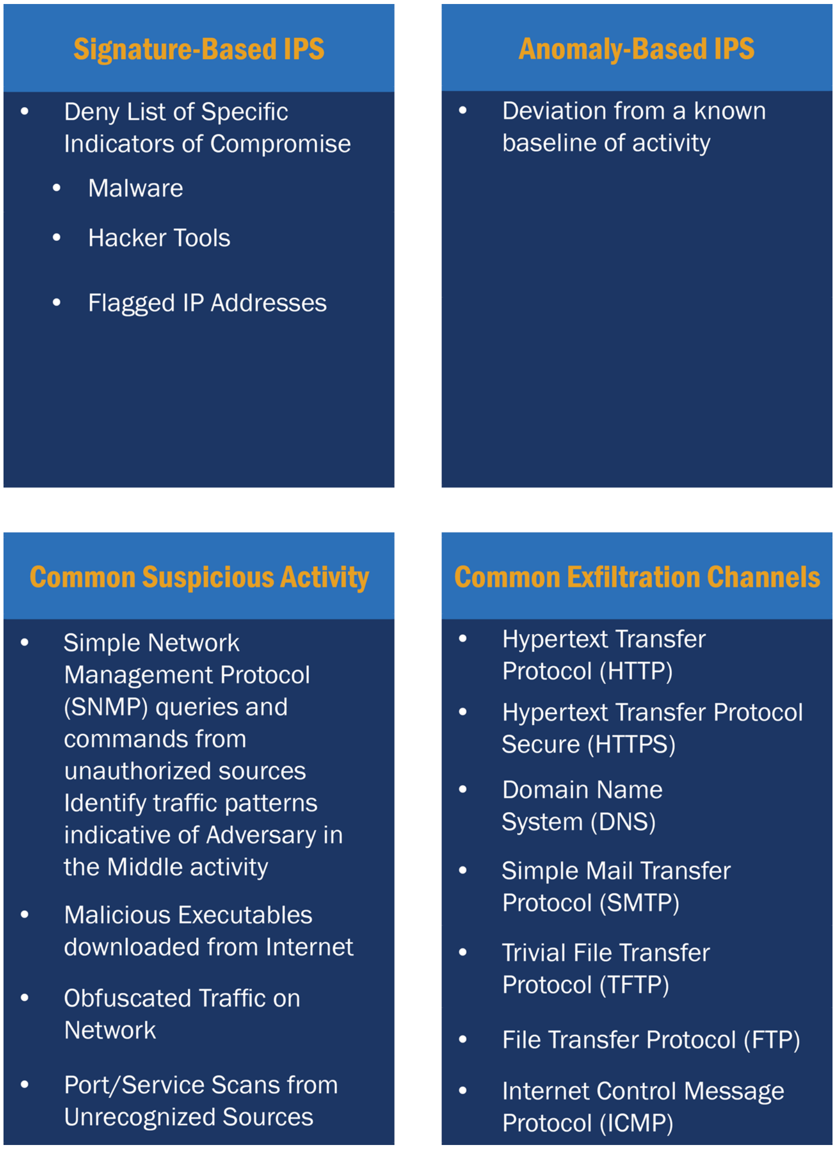
Terminal Operating Systems (TOS) are a common tool used at port facilities for managing the movement of cargo. Organizations configure these systems so data can be accessible to an Internet-facing web portal, inside the facility's enterprise network, and accessible from OT technology. Protect your TOS by securely configuring the system and all accounts used in conjunction with the TOS application.

- Protect your Service Accounts
- Enable AES Kerberos authentication
- Use complex 25+ character passwords for all service accounts (or any account with a Service Principal Name)
- Implement Group Managed Service Accounts
- Limit Service Accounts to only have permissions to run the necessary service
- Cycle the KRBTGT hash every 90 days


Terminal Operating System
Privileged credentials at risk if service account used for TOS database not hardened
Internet Accessible System at risk from unpatched vulnerabilities
Customer Portal
Domain Controller
TOS MSSQL
Gantry Cranes
Terminal Operating System

Common Mitigation #5: Network Intrusion Prevention

- Use signatures and anomaly detection to block malicious traffic



Signature-Based IPS

- Deny List of Specific Indicators of Compromise
  - Malware
  - Hacker Tools
  - Flagged IP Addresses

Anomaly-Based IPS

- Deviation from a known baseline of activity

Common Suspicious Activity

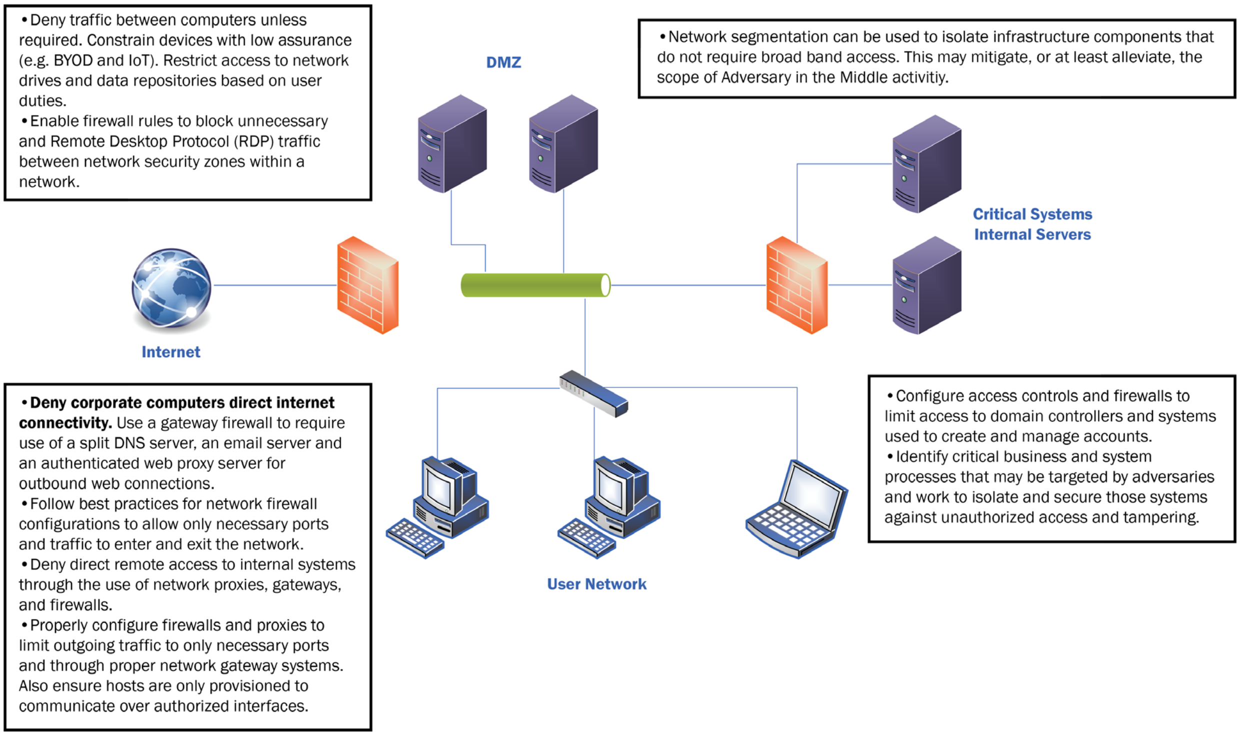
- Simple Network Management Protocol (SNMP) queries and commands from unauthorized sources Identify traffic patterns indicative of Adversary in the Middle activity
- Malicious Executables downloaded from Internet
- Obfuscated Traffic on Network
- Port/Service Scans from Unrecognized Sources

Common Exfiltration Channels

- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- Domain Name System (DNS)
- Simple Mail Transfer Protocol (SMTP)
- Trivial File Transfer Protocol (TFTP)
- File Transfer Protocol (FTP)
- Internet Control Message Protocol (ICMP)

Common Mitigation #6: Network Segmentation

- Design sections of the network to isolate critical systems, functions, or resources
- Use physical and logical segmentation to prevent access to potentially sensitive systems and information.
- A Demilitarized Zone (DMZ) contains Internet-facing services preventing exposure of the internal network to the Internet
- Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems



- Deny traffic between computers unless required. Constrain devices with low assurance (e.g. BYOD and IoT). Restrict access to network drives and data repositories based on user duties.
- Enable firewall rules to block unnecessary and Remote Desktop Protocol (RDP) traffic between network security zones within a network.

- Network segmentation can be used to isolate infrastructure components that do not require broad band access. This may mitigate, or at least alleviate, the scope of Adversary in the Middle activitiy.

- **Deny corporate computers direct internet connectivity.** Use a gateway firewall to require use of a split DNS server, an email server and an authenticated web proxy server for outbound web connections.
- Follow best practices for network firewall configurations to allow only necessary ports and traffic to enter and exit the network.
- Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.
- Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems. Also ensure hosts are only provisioned to communicate over authorized interfaces.

- Configure access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts.
- Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.

Common Mitigation #7: Vulnerability Scanning

- Use vulnerability scanning to find potentially exploitable software vulnerabilities to remediate them
  - Regularly scan externally facing systems and internal networks for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure
  - Implement continuous monitoring of vulnerability sources and the use of automatic and manual code review tools

Common Mitigation #8: Update Software

- Perform regular software updates to mitigate exploitation risk
  - Ensure operating systems and browsers are using the most current version
  - Update password managers regularly by employing patch management for internal enterprise endpoints and servers
  - Keep system images and software updated and migrate to SNMPv3
  - Update all browsers and plugins and use modern browsers with security features turned on
  - Update software regularly by employing patch management for externally exposed applications and internal enterprise endpoints and servers
  - Patch the BIOS and other firmware as necessary to prevent successful use of known vulnerabilities
  - Update software regularly to include patches that fix Dynamic Link Library (DLL) side-loading vulnerabilities

Common Mitigation #9: User Training

Password Reuse

- Don’t reuse the same password on multiple websites/applications

Drive-by Compromise

- Lock your computer and, if applicable, remove smart card when not in use

Credentials in Clear-text

- Don’t store passwords in unencrypted files

Spear-phishing Links

- Don’t click on unrecognized links

Spear-phishing Attachments

- Don’t open attachments from unrecognized senders

Domain Squatting

- Look out for websites with certificate errors, it may be a fake website

Credential Harvesting

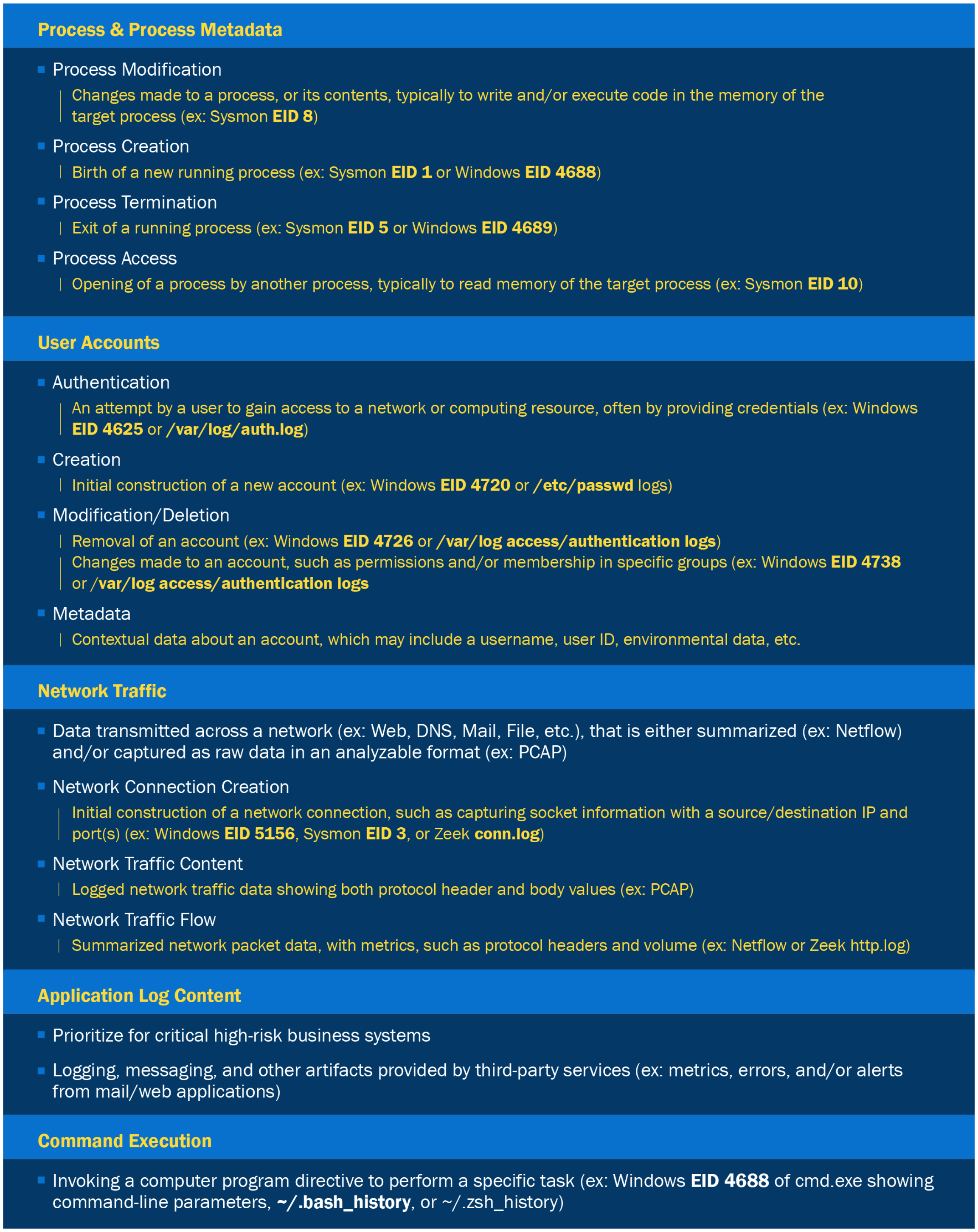
- Make sure you are on a legitimate site when entering a username/password

Unauthorized Applications

- Don’t use unauthorized applications without approval

Common Detections: Logging

In addition to mitigations, ATT&CK also provides detection recommendations. The below graphic summarizes the recommended detection techniques to successfully capture the ATT&CK techniques used in the attack path steps.



Process & Process Metadata

- Process Modification
  - Changes made to a process, or its contents, typically to write and/or execute code in the memory of the target process (ex: Sysmon **EID 8**)
- Process Creation
  - Birth of a new running process (ex: Sysmon **EID 1** or Windows **EID 4688**)
- Process Termination
  - Exit of a running process (ex: Sysmon **EID 5** or Windows **EID 4689**)
- Process Access
  - Opening of a process by another process, typically to read memory of the target process (ex: Sysmon **EID 10**)

User Accounts

- Authentication
  - An attempt by a user to gain access to a network or computing resource, often by providing credentials (ex: Windows **EID 4625** or **/var/log/auth.log**)
- Creation
  - Initial construction of a new account (ex: Windows **EID 4720** or **/etc/passwd** logs)
- Modification/Deletion
  - Removal of an account (ex: Windows **EID 4726** or **/var/log access/authentication logs**)
  - Changes made to an account, such as permissions and/or membership in specific groups (ex: Windows **EID 4738** or **/var/log access/authentication logs**
- Metadata
  - Contextual data about an account, which may include a username, user ID, environmental data, etc.

Network Traffic

- Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP)
- Network Connection Creation
  - Initial construction of a network connection, such as capturing socket information with a source/destination IP and port(s) (ex: Windows **EID 5156**, Sysmon **EID 3**, or Zeek **conn.log**)
- Network Traffic Content
  - Logged network traffic data showing both protocol header and body values (ex: PCAP)
- Network Traffic Flow
  - Summarized network packet data, with metrics, such as protocol headers and volume (ex: Netflow or Zeek http.log)

Application Log Content

- Prioritize for critical high-risk business systems
- Logging, messaging, and other artifacts provided by third-party services (ex: metrics, errors, and/or alerts from mail/web applications)

Command Execution

- Invoking a computer program directive to perform a specific task (ex: Windows **EID 4688** of cmd.exe showing command-line parameters, **~/.bash_history**, or ~/.zsh_history)

RECOMMENDED FURTHER ACTIONS

National Response Center (NRC)

The Coast Guard recommends that MTSA-regulated facilities and vessel owners/operators list the NRC's 24-hour hotline, **1-800-424-8802**, in their facility/vessel security plans for reporting maritime security and cybersecurity incidents to the Coast Guard. The NRC recommends all reports be made via this telephone hotline in order to record all pertinent information. The NRC no longer provides an email address on its website for reporting incidents. Additional reporting guidance is provided within Coast Guard Policy Letter 08-16, "Reporting Suspicious Activities and Breaches of Security." The policy letter outlines the requirements for MTSA-regulated vessels and facilities to report security incidents, in accordance with the 2002 Maritime Transportation Security Act.

Port Security Grants

The Port Security Grant Program (PSGP) is one of four grant programs that constitute DHS/Federal Emergency Management Agency's (FEMA) focus on transportation infrastructure security activities. These grant programs are part of a comprehensive set of measures authorized by Congress and implemented by the Administration to help strengthen the Nation's critical infrastructure. This includes grants for cybersecurity. Enhancing cybersecurity was identified as a priority area for Fiscal Year 2022 within the public "DHS Notice of Funding Opportunity (NOFO) Fiscal Year 2022 PSGP" published on **https://www.fema.gov/**. The PSGP provides funds to state, local, and private sector maritime partners to support increased port-wide risk management and protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies. The PSGP is subject to the annual appropriations process and awards project funding on a competitive basis across multiple priority areas, including cybersecurity.
Port Security Grant Program: https://www.fema.gov/grants/preparedness/port-security

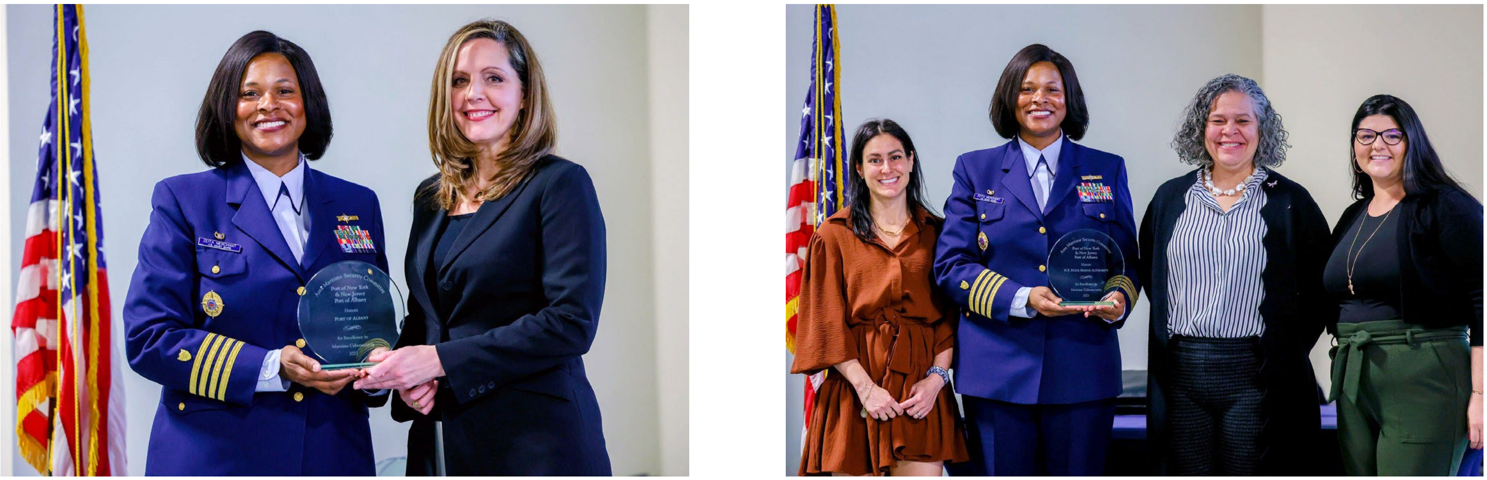
CISA's Cyber Hygiene Services

CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. https://www.cisa.gov/cyber-hygiene-services

- Vulnerability Scanning: Evaluates external network presence by executing continuous scans of public, static IPs for accessible services, and vulnerabilities. The service provides weekly vulnerability reports and ad-hoc alerts.
- Web Application Scanning: Evaluates known and discovered publicly accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- Phishing Campaign Assessment: Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support the measure of effectiveness of security awareness training.
- Remote Penetration Test: Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally available applications, and the potential for exploitation of open source information.

Additionally, CISA recommends you further protect your organization by identifying assets that are searchable via online tools and taking steps to reduce that exposure.

CYBERSECURITY EFFORTS AT COAST GUARD SECTOR NEW YORK



Captain Zeita Merchant, Sector Commander at Coast Guard Sector New York, presents port partners with award for "Excellence in Maritime Cybersecurity" at 2021 Sector New York Area Maritime Security Committee (AMSC) Member at Large Meeting.

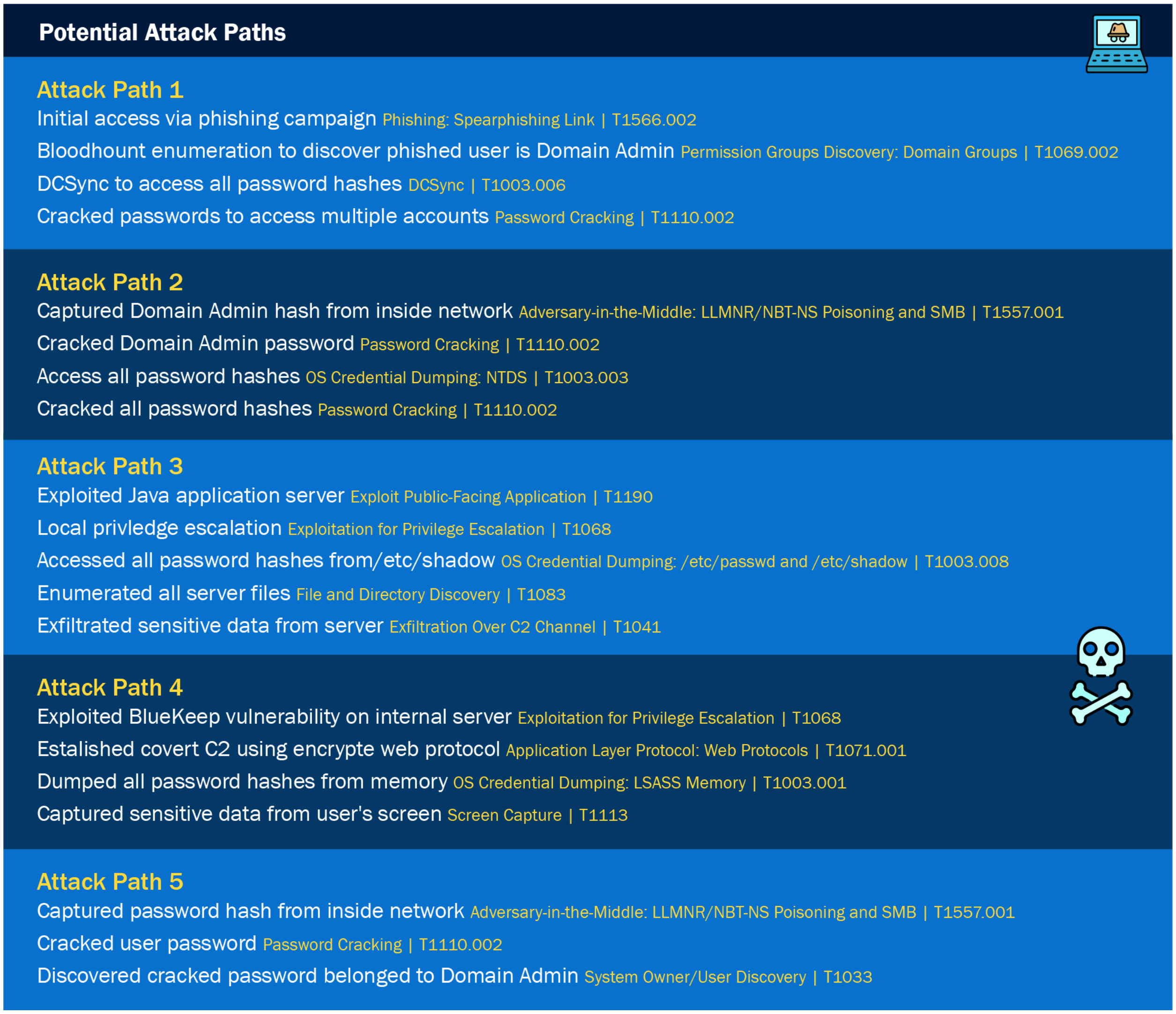
"Coast Guard Cyber Command's Cyber Protection Teams (CPT) provide marine transportation system (MTS) stakeholders access to highly trained and capable technical specialists across a spectrum of cyber protection capabilities. Sector New York has been highly successful leveraging the Area Maritime Security Committee to inform, educate, and advocate to partners concerning CPT's role in supporting the MTS. Anyone who has been around a Sector has heard the adage 'when prevention does their job we don't need response.' This is every bit the goal with cyber security. CPTs provide a robust and rapid suite of capabilities to respond to cyber disruptions, but once the '911' call is made, the impacts to supply chain and/or MTS are realized. The Coast Guard has taken its first steps into regulating cybersecurity at MTSA-regulated facilities with the implementation of NVIC 01-20, but we know MTS cyber threats extend beyond just MTSA facilities. Sector New York's approach to try to get ahead of cyber disruptions to supply chain and MTS is to prioritize specific sectors that, if disrupted, would have significant impacts to MTS at the local, regional, and national leve31. We directly advocated for those agencies and companies to work with a CPT for an assessment. We have had success, but the process is slow. Getting to 'yes' for an assessment takes time because we must build trust, transparency, and an understanding of what the CPT does. We are committed to the process and are finding partners that want to work with a CPT are very successful in Port Security Grant funding which helps bring more partners to the table. Sector New York will continue to use CPT resources to improve cyber resilience in one of the most import regions in the Nation."

- *Commander Kyle Weist, Emergency Management & Force Readiness Chief, Coast Guard Sector New York*

LTJG John "JL" Benton from 1790 Cyber Protection Team discusses CPT capabilities for Sector New York AMSC Members at Large.

APPENDIX A: POTENTIAL ATTACK PATHS

The below attack paths show the sequence of MITRE ATT&CK Techniques an MCA can use to advance through an organization's network.



Potential Attack Paths

Attack Path 1

Initial access via phishing campaign Phishing: Spearphishing Link | T1566.002

Bloodhount enumeration to discover phished user is Domain Admin Permission Groups Discovery: Domain Groups | T1069.002

DCSync to access all password hashes DCSync | T1003.006

Cracked passwords to access multiple accounts Password Cracking | T1110.002

Attack Path 2

Captured Domain Admin hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked Domain Admin password Password Cracking | T1110.002

Access all password hashes OS Credential Dumping: NTDS | T1003.003

Cracked all password hashes Password Cracking | T1110.002

Attack Path 3

Exploited Java application server Exploit Public-Facing Application | T1190

Local privledge escalation Exploitation for Privilege Escalation | T1068

Accessed all password hashes from/etc/shadow OS Credential Dumping: /etc/passwd and /etc/shadow | T1003.008

Enumerated all server files File and Directory Discovery | T1083

Exfiltrated sensitive data from server Exfiltration Over C2 Channel | T1041

Attack Path 4

Exploited BlueKeep vulnerability on internal server Exploitation for Privilege Escalation | T1068

Estalished covert C2 using encrypte web protocol Application Layer Protocol: Web Protocols | T1071.001

Dumped all password hashes from memory OS Credential Dumping: LSASS Memory | T1003.001

Captured sensitive data from user's screen Screen Capture | T1113

Attack Path 5

Captured password hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked user password Password Cracking | T1110.002

Discovered cracked password belonged to Domain Admin System Owner/User Discovery | T1033

Attack Path 6

Guessed password to access internal computer Password Policy Discovery | T1201

Captured Workstation Admin hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked Workstation Admin password Password Cracking | T1110.002

Accessed service account with weak password Steal or Forge Kerberos Tickets: Kerberoasting | T1558.003

Cracked password for service account with Domain Admin permissions Password Cracking | T1110.002

Attack Path 7

Guessed password to access internal computer Password Policy Discovery | T1201

Captured Workstation Admin hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked Workstation Admin password Password Cracking | T1110.002

Discovered improperly configured setting Permission Groups Discovery: Domain Groups | T1069.002

DCSYNC all DCSync | T1003.006

Access backup service with default credentials Valid Accounts: Default Accounts | T1078.001

Simulated ransomware attack Data Encrypted for Impact | T1486

Attack Path 8

Default password to public web app Valid Accounts: Default Accounts | T1078.001

Ran malicious code from admin interface Exploit Public-Facing Application | T1190

Estalished covert C2 using encrypted web protocol Application Layer Protocol: Web Protocols | T1071.001

Discovered full administrative access to system from exploit System Owner/User Discovery | T1033

Attack Path 9

Captured password hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked user password Password Cracking | T1110.002

Enumerated system files System Owner/User Discovery | T1033

Discovered password in file Unsecured Credentials: Credentials In Files | T1552.001

Determined account had access to database used by OT systems Valid Accounts: Domain Accounts | T1078.002

Used account to create a web shell to access OT system Server Software Component: Web Shell | T1505.003

Created remote access to OT system database over encrypted web traffic Application Layer Protocol: Web Protocols | T1071.001

Dumped all password hashes from memory OS Credential Dumping: LSASS Memory | T1003.001

Attack Path 10

Captured Domain Admin hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked Domain Admin password Password Cracking | T1110.002

Validated local admin permissions System Owner/User Discovery | T1033

Validated Domain Admin permissions Permission Groups Discovery: Domain Groups | T1069.002

Access all password hashes OS Credential Dumping: NTDS | T1003.003

Cracked all password hashes Password Cracking | T1110.002

Attack Path 11

Captured password hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked user password Password Cracking | T1110.002

Discovered user permissions as Local Administrator of another computer System Owner/User Discovery | T1033

Dumped all password hashes from memory OS Credential Dumping: LSASS Memory | T1003.001

Cracked user password Password Cracking | T1110.002

Discovered 2nd user permissions as Local Administrator of another computer System Owner/User Discovery | T1033

Dumped all password hashes from memory OS Credential Dumping: LSASS Memory | T1003.001

Cracked user password Password Cracking | T1110.002

Attack Path 12

Captured password hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked user password Password Cracking | T1110.002

Discovered cracked password belonged to Domain Admin Permission Groups Discovery: Domain Groups | T1069.002

Access all password hashes OS Credential Dumping: NTDS | T1003.003

Cracked all password hashes Password Cracking | T1110.002

Attack Path 13

Added malicious commands to internal network traffic Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Estalished covert C2 using encrypted web protocol Application Layer Protocol: Web Protocols | T1071.001

Dumped all password hashes from memory OS Credential Dumping: LSA Secrets | T1003.004

Used administrator password hash to connnect to remote workstation as Admin Use Alternate Authentication Material: Pass the Hash | T1550.002

Attack Path 14

Exploited email server vulnerability Exploit Public-Facing Application | T1190

Created publicly available web shell for administrative access to server Server Software Component: Web Shell | T1505.003

Attack Path 15

Exploited zero day exploit on public web app Exploit Public-Facing Application | T1190

Uploaded malicious payload for persistence Exploitation for Client Execution | T1203

Enumerated current user System Owner/User Discovery | T1033

Enumerate all Domain Admins & VPN users Permission Groups Discovery: Domain Groups | T1069.002

Switched to active Domain Admin account Unsecured Credentials: Credentials in Registry | T1552.002

Dumped all password hashes OS Credential Dumping: NTDS | T1003.003

Moved all password hashes to web directory Exfiltration Over Web Service: Exfiltration to Cloud Storage | T1567.002

Switched to active Domain Admin account Unsecured Credentials: Credentials in Registry | T1552.002

Accessed facility access control system System Owner/User Discovery | T1033

Attack Path 16

Malicious content opened in email Phishing: Spearphishing Link | T1566.002

Dumped all password hashes from memory OS Credential Dumping: LSASS Memory | T1003.001

Disabled antivirus Impair Defenses: Disable or Modify Tools | T1562.001

Used password hashes to access administrator account Use Alternate Authentication Material: Pass the Ticket | T1550.003

Deployed ransomware throughout network Data Encrypted for Impact | T1486

Attack Path 17

Success phishing email clicked by user Phishing: Spearphishing Link | T1566.002

Estalished covert C2 using encrypted web protocol Application Layer Protocol: Web Protocols | T1071.001

Accessed domain groups and permissions Permission Groups Discovery: Domain Groups | T1069.002

Attempted common passwords against admin accounts Brute Force: Password Spraying | T1110.003

Valid login as Domain Admin Valid Accounts: Domain Accounts | T1078.002

Attack Path 18

Captured password hash from inside network Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB | T1557.001

Cracked user password Password Cracking | T1110.002

Utilzed valid account to discover service accounts Permission Groups Discovery: Domain Groups | T1069.002

Accessed service account password hash with weak password Steal or Forge Kerberos Tickets: Kerberoasting | T1558.003

Cracked service account password Password Cracking | T1110.002

Created access token as service account Steal or Forge Kerberos Tickets: Golden Ticket | T1558.001

APPENDIX B: BADALLOC CRITICAL VULNERABILITY: BLACKBERRY ONX & MORE

US Coast Guard Cyber Command
Maritime Cyber Alert 02-21

August 17, 2021

Information Sharing Protocol: TLP-White (https://www.us-cert.gov/tlp)

“BADALLOC” CRITICAL VULNERABILITY: BLACKBERRY QNX & MORE

Summary:
The recent public disclosure from BlackBerry regarding the “BadAlloc” vulnerability in their QNX OS versions 6.5 and earlier, should put all organizations on continued alert for threats and vulnerabilities to the cyber landscape. “BadAlloc” is the name assigned to the family of vulnerabilities discovered in embedded Internet of Things (IoT) and Operational Technology (OT) operating systems and software to describe a class of memory overflow vulnerabilities.

An embedded system is a computer implemented as part of a larger system. It is typically designed around a limited set of specific functions in relation to the larger system and it may consist of the same components of a typical computer, or be just a microcontroller.

A device with these exploitable vulnerabilities may enable malicious actors to deny system availability, ex-filtrate data, and move laterally within the systems in which they are installed. These malicious actions can lead to consequences for systems and their users, ranging from loss of data and trust, to physical harm and loss of life.

BlackBerry QNX is the most recent organization to disclose this vulnerability, however there are several other products that have the same “BadAlloc” vulnerability. The Maritime community should be examining their systems to determine if they contain BlackBerry QNX versions 6.5 or below, or any of the other products identified by CISA listed in ICSA-21-119-04: Multiple RTOS (Update B).

Mitigations:

There are two significant challenges with mitigating this vulnerability. The first is identifying the systems and products that have vulnerable software. Because this vulnerability is most prevalent in embedded systems, it may not be readily apparent that your organization has this vulnerability. Each organization is strongly encouraged to extensively review their systems and to identify any that contain vulnerable software/operating systems.

The second challenge relates to applying updates. The best solution for mitigating this vulnerability is upgrading to a new, non-vulnerable version. For example, upgrading QNX to version 6.6 or higher mitigates the vulnerability. However, many of the systems running QNX and these other real-time operating systems (RTOS) vulnerable software may be difficult to upgrade due to required downtime.

If you are able, the best mitigation is to upgrade to a secure version of the vendor's software, but before doing so, first compute the hash values of the upgraded software and verify that they match the values published by the vendors. Additionally, thoroughly test the upgraded software in a sandboxed environment on isolated devices to ensure that the new software does not negatively affect or render inoperable any devices that it will be loaded on and interact.

If operations do not permit the downtime required to apply the needed upgrade, or an upgrade is not available, it is recommended that appropriate controls are identified and implemented to mitigate the risks. Potential controls may include:

- Limiting remote access to the vulnerable devices, and understanding even "secure" methods such as Virtual Private Networks may have other vulnerabilities.
- Ensuring vulnerable devices are not accessible from the internet.
- Placing vulnerable control system networks and remote devices behind firewalls and isolating them from business networks.

Additionally, it is recommended to not only implement controls to protect from exploitation, but ensure that software and hardware inventory policies are current and adequate. Quick identification of vulnerable systems is critical to prevent threat actors from damaging critical systems. Many applications and devices may run on QNX, but require research to confirm if this vulnerability is present. A complete understanding of components that make up your critical systems, and a comprehensive inventory will assist in quickly identifying risks to your organization.

Resources:

If your organization identifies a vulnerability or has any questions related to this alert, such as technical assistance with the mitigation actions, please contact U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.

The information contained in this cyber alert is provided for informational purposes only. This information is based on common standards and best practices, and the implementation of which does not relieve any domestic, international safety, operational, or material requirements. The USCG does not provide any warranties of any kind regarding this information and shall not be held liable for any damages of any kind that arose out of the results of, or reliance upon this information.

APPENDIX C: ACTIVELY EXPLOITED CRITICAL VULNERABILITY IN APACHE LOG4J

US Coast Guard Cyber Command
Maritime Cyber Alert 04-21

December 15, 2021

Information Sharing Protocol: TLP-White (https://www.us-cert.gov/tlp)

Actively Exploited Critical Vulnerability in Apache Log4j

Summary:

This Maritime Cyber Alert (MCA) identifies critical vulnerability CVE-2021-44228, rated 10 out of 10 on the Common Vulnerability Scoring System (CVSS) by the National Institute of Standards and Technology. This critical vulnerability affects a ubiquitous logging tool used in the vast majority of Java applications. Numerous types of applications are built using Java including mobile apps, web servers, enterprise applications, embedded systems, and distributed applications. It is estimated more than 100 million devices world-wide across every industry, including the Marine Transportation System (MTS), are impacted. All organizations are urged to take immediate action in order to identify and mitigate this vulnerability.

This vulnerability is:

- **Easy to Exploit** – Exploitation is only 12 characters long, and there are a vast number of proof of concepts that are already public.
- **Rapid Automation** – The simplicity of the exploit makes it easy for attackers to automate exploitation.
- **No Network Access or Privilege Restrictions** – Enables the attacker to run remote code execution on a device without any authentication, granting the attacker full control of a system or device.

An unsophisticated remote attacker could exploit this vulnerability to take full control of an affected system.

The following versions are affected: Log4j versions 2.0-beta9 to 2.14.1.

The first known indicator of compromise related to this vulnerability dates back to December 1st, 2021, but it is currently unclear which threat actors are exploiting it. The Cybersecurity and Infrastructure Security Agency (CISA) created a page to be the authoritative source for information related to this vulnerability. Organizations that identify they are vulnerable are strongly encouraged to regularly check the CISA site for updates on indicators of compromise and mitigation tactics for the foreseeable future.

Mitigations:

There are four recommended steps to mitigate:

1) Scan applications to identify what systems are using vulnerable versions of Log4j. Several free tools are available that can assist with scanning. It is not always readily apparent what systems are using Log4j. Prioritize mitigating public facing applications and critical systems first. However, all vulnerable systems are exploitable and need remediation.
2) Upgrade to Log4j 2.15.0 or later. If you are unable to upgrade, certain versions may allow you to take alternative steps to mitigate the vulnerability.
3) Ensure your security operations center is acting on every alert on systems that are running vulnerable versions of Log4j, even after patching. Review all logs dating back to at least 1 December 2021 to identify potential malicious activity.
4) Update Web Application Firewalls with newest rules. This may prevent attackers using mass scanning and other unsophisticated techniques.

There are still a lot of unknowns related to this vulnerability and organizations are strongly encouraged to continue to check with authoritative sources for new information. Patching may correct this vulnerability, but that alone may not fully protect your organization from compromise.

Resources:

If your organization identifies a vulnerability or has any questions related to this alert, please contact U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.

The information contained in this cyber alert is provided for informational purposes only. This information is based on common standards and best practices, and the implementation of which does not relieve any domestic, international safety, operational, or material requirements. The USCG does not provide any warranties of any kind regarding this information and shall not be held liable for any damages of any kind that arose out of the results of, or reliance upon this information.

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-259A

September 16, 2021

APPENDIX D: APT ACTORS EXPLOITING NEWLY IDENTIFIED VULNERABILITY IN MANAGEENGINE ADSELFSERVICE PLUS 0

SUMMARY

This joint advisory is the result of analytic efforts between the FBI, United States Coast Guard Cyber Command (CGCYBE and the Cybersecurity And Infrastructure Security Agency (CISA) to highlight the Cyber threat associated with active exploitation of a newly Identified vulnerability (CVE-2021-40539 in ManageEngine ADSelfService Plus – a self-service password management and single sign-on solution.

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the [ATT&CK for Enterprise framework]() for referenced threat actor techniques and for mitigations.

CVE-2021-40539, rated critical by the Common Vulnerability Scoring System (CVSS) is an authentication bypass vulnerability affecting representational state transfer (REST) application programming interface (API) URLs that could enable remote code execution. The FBI, CISA, and CGCUBER assess that advanced persistent threat (APT) cyber actors are likely among those exploiting the vulnerability. The exploitation of ManageEngine ADSelfService Plus poses a series risk to critical infrastructure companies, U.S. – cleared defense contractors, academic institutions, and other entities that use the software. Successful exploitation of the vulnerability allows an attacker to place web shells, which enable the adversary to conduct post-exploitation activities, such as compromising administrator credentials, conducting lateral movement, and exfiltrating registry hives and Active Directory files.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contactyour local FBI field office at https://www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov. To report cyber incidents to the Coast Guard pursuant to 33 CFR Subchapter H, Part 101.305 please contact the USCG National Response Center (NRC) Phone: 1-800-424- 8802, email: NRC@uscg.mil.

Disclaimer: *The information in this Joint Cybersecurity Advisory is provided "as is" for informational purposes only. FBI and CISA do not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis. This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/.*

Zoho ManageEngine ADSelfService Plus build 6114, which Zoho released on September 6, 2021, fixes CVE-2021-40539. FBI, CISA, and CGCYBER strongly urge users and administrators to updateto ADSelfService Plus build 6114. Additionally, FBI, CISA, and CGCYBER strongly urge organizations ensure ADSelfService Plus is not directly accessible from the internet.

The FBI, CISA, and CGCYBER have reports of malicious cyber actors using exploits against CVE- 2021-40539 to gain access [T1190] to ManageEngine ADSelfService Plus, as early as August 2021.The actors have been observed using various tactics, techniques, and procedures (TTPs), including:

- Frequently writing webshells [T1505.003] to disk for initial persistence
- Obfuscating and Deobfuscating/Decoding Files or Information [T1027 and T1140]
- Conducting further operations to dump user credentials [T1003]
- Living off the land by only using signed Windows binaries for follow-on actions [T1218]
- Adding/deleting user accounts as needed [T1136]
- Stealing copies of the Active Directory database (`NTDS.dit`) [T1003.003] or registry hives
- Using Windows Management Instrumentation (WMI) for remote execution [T1047]
- Deleting files to remove indicators from the host [T1070.004]
- Discovering domain accounts with the `net` Windows command [1087.002]
- Using Windows utilities to collect and archive files for exfiltration [T1560.001]
- Using custom symmetric encryption for command and control (C2) [T1573.001]

The FBI, CISA, and CGCYBER are proactively investigating and responding to this malicious cyberactivity.

- FBI is leveraging specially trained cyber squads in each of its 56 field offices and CyWatch, the FBI's 24/7 operations center and watch floor, which provides around-the-clock support totrack incidents and communicate with field offices across the country and partner agencies.
- CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify,and reduce their exposure to threats. By requesting these services, organizations of any sizecould find ways to reduce their risk and mitigate attack vectors.
- CGCYBER has deployable elements that provide cyber capability to marine transportationsystem critical infrastructure in proactive defense or response to incidents.

Sharing technical and/or qualitative information with the FBI, CISA, and CGCYBER helps empowerand amplify our capabilities as federal partners to collect and share intelligence and engage with victims while working to unmask and hold accountable, those conducting malicious cyber activities.See the Contact section below for details.

TECHNICAL DETAILS

Successful compromise of ManageEngine ADSelfService Plus, via exploitation of CVE-2021-40539,allows the attacker to upload a `.zip` file containing a Java Server Pages (JSP) web shell masquerading as an x509 certificate: `service.cer`. Subsequent requests are then made to differentAPI endpoints to further exploit the victim's system.

After the initial exploitation, the JSP web shell is accessible at `/help/admin-guide/Reports/ReportGenerate.jsp`. The attacker then attempts to move laterally using Windows Management Instrumentation (WMI), gain access to a domain controller, dump `NTDS.dit` and `SECURITY/SYSTEM` registry hives, and then, from there, continues the compromised access.

Confirming a successful compromise of ManageEngine ADSelfService Plus may be difficult—the attackers run clean-up scripts designed to remove traces of the initial point of compromise and hideany relationship between exploitation of the vulnerability and the web shell.

(Updated November 19, 2021): APT actors are using the following suite of tools to enable this campaign:

- Dropper – a dropper Trojan that drops Godzilla web shell on a system.
- Godzilla – a Chinese language web shell.
- NGLite – a backdoor Trojan written in Go.
- KdcSponge – a credential-stealing tool that targets undocumented APIs in Microsoft's implementation of Kerberos.

The FBI, CISA, and CGCYBER cannot confirm the CVE-2021-40539 is the only vulnerability APT actors are leveraging as part of this activity, so it is key that network defenders focus on detecting thetools listed above in addition to initial access vector. For more information, see:

- Palo Alto Networks blog post: KdcSponge, NGLite, Godzilla Webshell Used in Targeted AttackCampaign.
- Microsoft Security blog post: Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus.
- IBM Security Intelligence blog post: Call to Patch: Zero Day Discovered in Enterprise HelpDesk Platform.

Note: The FBI, CISA, and CGCYBER do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement,recommendation, or favoring by the FBI, CISA, and CGCYBER. This document does not change anylegal requirements or impose new requirements on the public.

Targeted Sectors

APT cyber actors have targeted entities across the 16 critical infrastructure sectors, including academic institutions, defense contractors, as well as transportation, information technology, manufacturing, communications, and finance. Illicitly obtained access and information may disruptcompany operations/logistics and subvert U.S. research across critical infrastructure sectors.

Indicators of Compromise

Hashes:

`068d1b3813489e41116867729504c40019ff2b1fe32aab4716d429780e666324`

`49a6f77d380512b274baff4f78783f54cb962e2a8a5e238a453058a351fcfbba`

File paths:

```
C:\ManageEngine\ADSelfService Plus\webapps\adssp\help\admin-
guide\reports\ReportGenerate.jsp
C:\ManageEngine\ADSelfService Plus\webapps\adssp\html\promotion\adap.jsp
C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\help
C:\ManageEngine\ADSelfService Plus\jre\bin\SelfSe~1.key (filename varies with anepoch
timestamp of creation, extension may vary as well) C:\ManageEngine\ADSelfService
Plus\webapps\adssp\Certificates\SelfService.csr C:\ManageEngine\ADSelfService
Plus\bin\service.cer
C:\Users\Public\custom.txt C:\Users\Public\custom.bat
C:\ManageEngine\ADSelfService
Plus\work\Catalina\localhost\ROOT\org\apache\jsp\help (including subdirectoriesand
contained files)
```

Web shell URL Paths:

`/help/admin-guide/Reports/ReportGenerate.jsp`

`/html/promotion/adap.jsp`

Check log files located at `C:\ManageEngine\ADSelfService Plus\logs` for evidence of successful exploitation of the ADSelfService Plus vulnerability:

- In access* logs:
  - `/help/admin-guide/Reports/ReportGenerate.jsp`
  - `/ServletApi/../RestApi/LogonCustomization`
  - `/ServletApi/../RestAPI/Connection`
- In serverOut_* logs:
  - `Keystore will be created for "admin"`
  - `The status of keystore creation is Upload!`
- In adslog* logs:
  - Java traceback errors that include references to NullPointerException in addSmartCardConfig or `getSmartCardConfig`

TTPs:

- WMI for lateral movement and remote code execution (`wmic.exe`)
- Using plaintext credentials acquired from compromised ADSelfService Plus host

- Using `pg_dump.exe` to dump ManageEngine databases
- Dumping `NTDS.dit` and `SECURITY/SYSTEM/NTUSER` registry hives
- Exfiltration through web shells
- Post-exploitation activity conducted with compromised U.S. infrastructure
- Deleting specific, filtered log lines

Yara Rules:

```
rule ReportGenerate_jsp {
   strings:
            $s1 = "decrypt(fpath)"
            $s2 = "decrypt(fcontext)"
            $s3 = "decrypt(commandEnc)"
            $s4 = "upload failed!"
```

```
   condition:
            filesize < 15KB and 4 of them
      }
```

```
rule EncryptJSP {
   strings:
            $s1 = "AEScrypt"
            $s2 = "AES/CBC/PKCS5Padding"
            $s3 = "SecretKeySpec"
            $s4 = "FileOutputStream"
            $s5 = "getParameter"
```

```
            $s8 = "readLine()"
   condition:
            filesize < 15KB and 6 of them
      }
```

MITIGATIONS

Organizations that identify any activity related to ManageEngine ADSelfService Plus indicators ofcompromise within their networks should take action immediately.

Zoho ManageEngine ADSelfService Plus build 6114, which Zoho released on September 6, 2021, fixes CVE-2021-40539. FBI, CISA, and CGCYBER strongly urge users and administrators to updateto ADSelfService Plus build 6114. Additionally, FBI, CISA, and CGCYBER strongly urge organizations ensure ADSelfService Plus is not directly accessible from the internet.

Additionally, FBI, CISA, and CGCYBER strongly recommend domain-wide password resets anddouble Kerberos Ticket Granting Ticket (TGT) password resets if any indication is found that the `NTDS.dit` file was compromised.

Actions for Affected Organizations

Immediately report as an incident to CISA or the FBI (refer to Contact information section below) theexistence of any of the following:

- Identification of indicators of compromise as outlined above.
- Presence of web shell code on compromised ManageEngine ADSelfService Plus servers.
- Unauthorized access to or use of accounts.
- Evidence of lateral movement by malicious actors with access to compromised systems.
- Other indicators of unauthorized access or compromise.

CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that they may haverelated to this threat. For any questions related to this report or to report an intrusion and request resources for incidentresponse or technical assistance, please contact:

- To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at https://www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. Whenavailable, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- To request incident response resources or technical assistance related to these threats, contactCISA at Central@cisa.gov.
- To report cyber incidents to the Coast Guard pursuant to 33 CFR Section 101.305, please contact the USCG National Response Center (NRC) Phone: 1-800-424-8802.

APPENDIX E: LIST OF ACRONYMS

ADFS	Active Directory Federation Services
AOR	Area of Responsibility
API	Application Programming Interface
APWG	Anti-Phishing Working Group
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BIOS	Basic Input/output System
BOS	Breach of Security
C2	Command and Control
CGCYBER	United States Coast Guard Cyber Command
CIC	Critical Incident Communication
CI/KR	Critical Infrastructure & Key Resources
CISA	Cybersecurity and Infrastructure Security Agency
COTP	Captain of the Port
CPT	Cyber Protection Team
CSP	Credential Service Provider
CVSS	Common Vulnerability Scoring System
CY21	Calendar Year 2021
DCOM	Distributed Component Object Model
DLL	Dynamic Link Library
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
FEMA	Federal Emergency Management Agency
FBI	Federal Bureau of Investigation
FIR	Field Incident Report
FTP	File Transfer Protocol
GOS	Gate Operating System
HIRT	Hunt and Incident Response Team
HTTP	Hypertext Transfer Protocol Secure
IOT	Internet of Things
IP	Internet Protocol
IT	Information Technology
JSP	Java Server Page
MARSEC	Maritime Security
MCAs	Malicious Cyber Actors
MCRB	Maritime Cyber Readiness Branch
ME	Marine Environment
MFA	Multi-Factor Authentication
MTS	Marine Transportation System
MTSA	Marine Transportation Security Act
NIST	National Institute of Stands & Technology
NRC	National Response Center
NVIC	Navigation and Vessel Inspection Circular
OT	Operational Technology
OTP	One Time Password
PSGP	Port Security Grant Program

RaaS	Ransomware as a Service
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RVA	Risk & Vulnerability Assessment
SLTT	State, Local, Territorial, and Tribal
SNMP	Simple Network Management Protocol
SRMA	Sector Risk Management Agency
TFTP	Trivial File Transfer Protocol
TGT	Ticket Granting Ticket
TOS	Terminal Operating System
TSI	Transportation Security Incidents
TTP	Tactics, Techniques, & Procedures
URL	Uniform Resource Locator
VPC	Virtual Private Cloud
VPS	Virtual Private Servers
WinRM	Windows Remote Management