NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
July 2022 (Edition 2022-07)

This **electronic** publication is intended to inform port stakeholders about cyber security issues and provide information useful to safeguard seaport systems that may be vulnerable to cyber-attacks. The information contained herein is suitable for general release and members of the Northern California Area Maritime Security Committee are encouraged to pass it on to members of our maritime community. This newsletter will be e-mailed to members of the Northern California Area Maritime Security Committee and posted on the Coast Guard's HOMEPORT portal within the Sector San Francisco port area.

IF YOU SEE SOMETHING, SAY SOMETHING

To report a crime in progress, call 911 or your local police department. To report maritime related suspicious activities or breaches of security call the National Response Center (NRC) at 800-424-8802 or if a **cyber-attack** to the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870. After calling the NRC or NCCIC call the Captain of the Port, San Francisco, at 415-399-3530.

TABLE OF CONTENTS

ARTICLE SUMMARIES

- **Maritime Cybersecurity in 2022 –** discusses current trends and the need for good cybersecurity hygiene practices within a company’s workforce.
- **USCG MSIB 20-2022 –** discusses the need for continued vigilance and CISA’s “Shields Up” website as a place for information and reporting.
- **CSIA Alert AA22-137A – “**Weak Security Controls and Practices Routinely Exploited for Initial Access” discusses weaknesses in a system through misconfiguration or not upgraded. Hackers routinely exploit such systems.

MAIN ARTICLES

Maritime Cybersecurity in 2022, Brian Waltermire, 28MAR2022

Maritime Cyber Security

Tools, policies, security solutions, and industry standards for securing marine enterprises and their vessels as well as their IT environment are all included in maritime cybersecurity. Issues of data privacy and security are of paramount importance in today's quickly devolving cyber world. Even huge IT firms that are building complicated software and hardware solutions, Internet platforms, and IoT (Internet of Things) devices may not be able to guarantee the requisite degree of protection. Data breaches and leaks from major tech corporations like Twitter, Garmin, and Intel and other industrial giants have become common knowledge after they were breached in the year 2020. Everyone may not be affected by tech company hacks but as we've seen in the past two years everyone is affected by disruptions in the cargo shipping industry.

At present, the marine transportation sector provides one-fourth of the US GDP, or around $5.4 trillion, dollars. It's impossible to run a global supply chain without relying on marine transportation. Around 80% of global commerce volume was transported by sea and ports outside the United States in 2013. Trade by sea grew by 4% worldwide in 2018, the greatest rate of increase in the previous five years, in 2018.

Maritime Cybersecurity Challenges

The marine industry has many of the same cybersecurity concerns as other industries that engage with computer networks, including:

- All of the systems and devices on the OT network are not well-understood by everyone in the fleet or business.

- The lack of information about each ship's OT networks.

- Over time, an OT network that can't be watched in real time or divided into smaller parts creates risks.

- When IT and OT networks are accidentally linked together by mistake.

- Secure identity access and zero trust networking isn't widely implemented on third-party networks for OEMs.

- Poor or nonexistent communication tools between ports for information sharing increases likelihood of broader attacks.

Potential maritime Cybersecurity Attacks

When it comes to cyber security, it's not only about keeping hackers from getting into your systems and data. Digital assets and data must be safeguarded, operations must continue, and the marine sector must be robust to both internal and external threats. It is essential that ship systems be protected from physical assault and that supporting systems be kept in good working condition.

High-impact assaults against warships and tankers are possible because of their complexity. Incidents across the internet like DDoS attacks may persist for minutes, hours, or weeks rendering critical operations obsolete. Additionally, when a vessel's corporate network is compromised, malware may be distributed to other boats in the fleet. Operational failures may be slowed by a variety of threats, including:

- An attack on a satellite provider that obtains access to a ship's IT/OT network.

- An attack on an OEM or third-party network that extends to its client's on-vessel OT network.

- On-board computer systems (OT) may be compromised by exploiting cyber vulnerabilities that allow for a wide range of attacks on systems, such as:

o GPS/navigation system hacking is possible.

o Crucial valves must be opened and closed.

o Propulsion and rudder control are two separate functions.

o Controls for the halogen lamps.

o Ransomware/Malware.

Recent Maritime Cybersecurity Attacks

Currently more than 51,000 commercial ships are in operation around the world accounting for 90% of global trade.

Maersk, the world's largest container shipping company, was the victim of a particularly severe cyberattack in 2017. More than $450 million in damages were caused by the Not Petya virus that infected the company's 4500 computers worldwide. A German-owned container ship was allegedly taken over by hackers in February 2017. "Pirates" took control of the ship's navigation system and used it for 10 hours to steer it to a location where they could board and seize it. A single example of what can go wrong when exploiting a ship's systems and the company that operates them. If proactive measures aren't taken to address these issues, they will become more common in this new age of information technology in marine logistics.

Prevention against Maritime Cybersecurity attacks

Addressing maritime cybersecurity is a matter of the utmost importance. Listed below are a few general approaches for dealing with it:

- Recognize the threat environment encompassing the ship's internal IT and OT.

- Improve security by taking detailed inventories of onboard systems and running mock scenarios as if they were under a cyber-attack.

- Find out how likely it is that a vulnerability will be used by someone outside or inside the company.

- Make it less likely and more difficult for a potential vulnerability to be used by putting in monitored protection and detection measures like EDR.

- Develop and enforce high-priority contingencies to deal with any cyber risks that have been found.

- If there is a cyber-attack, the contingency plan should be used to enact a tested response and recover the system or data in line with RTO.

An important operational need in the marine environment of the twenty-first century is maintaining good cybersecurity, according to the U.S. Coast Guard's security alert issued in July of this year [actually July 2020].

Conclusion

More than 80% of data breaches are caused by human error, which is why cyber threats continue to grow in number. In the marine business, where ships and employees are continuously on the move, developing a cyber awareness defense becomes much more difficult. Education and awareness are essential if we are to reduce the danger of unauthorized access to and misuse of our data. It doesn't matter how advanced the technology is if the individuals who use it aren't properly educated and informed of the hazards. Because of this, it is essential to teach seafarers how to use information technology systems, including secure communication methods for collaborating, communicating and sharing the latest findings amongst themselves.

MSIB 20-2022, USCG, 15APR2022

The Coast Guard continues to monitor world events and their potential impact on the Marine Transportation System (MTS). We remain engaged with our interagency partners and industry stakeholders to share information and coordinate the federal government's preparedness and response efforts to minimize disruptions to the MTS, including disruptions due to cyber threats.

CISA's "Shields Up" website remains the primary location for information and recommendations for adapting a heightened cybersecurity posture, and we highly encourage all MTS stakeholders to visit the site regularly for updates and reminders. MTS stakeholders can also receive CISA's subscription service for timely updates/bulletins. The Coast Guard continues to monitor guidance and products from CISA and partner agencies and will distribute these materials to stakeholders, along with maritime- specific context, as appropriate

Per CISA’s “Shields Up” guidance, “Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. Government. In this heightened threat environment, these thresholds should be significantly lower than normal.” The Coast Guard fully supports this guidance and stands ready with our partner agencies to respond to these reports. Considering the heightened risk, stakeholders should closely monitor their computer systems, telecommunications systems, and networks for suspicious activity and breaches of security and, when in doubt, report to the National Response Center (NRC). Maritime Transportation Security Act (MTSA) regulated vessels and facilities are required, and other MTS stakeholders are encouraged, to report breaches of security or suspicious activity to the NRC at 1-800-424-8802. The CG-5P Policy Letter 08- 16, Reporting Suspicious Activity and Breaches of Security provides additional guidance on the reporting of cyber incidents

While breaches of security and suspicious activity are required to be reported to the NRC, the Coast Guard’s Cyber Command is available to provide technical support to help MTS stakeholders prepare for or respond to a cyber-incident. Their 24×7 watch can be reached at: 202-372-2904 or CGCYBER-SMB- NOSC-BWC@uscg.mil.

Thank you for your continued vigilance.
John W. Mauger, RADM, U. S. Coast Guard, Assistant Commandant for Prevention Policy sends.

Alert AA22-137A, CISA, 17MAY2022

Alert (AA22-137A) Weak Security Controls and Practices Routinely Exploited for Initial Access

SUMMARY

Best Practices to Protect Your Systems:
- Control access.
- Harden Credentials.
- Establish centralized log management.
- Use antivirus solutions.
- Employ detection tools.
- Operate services exposed on internet-accessible hosts with secure configurations.
- Keep software updated.

Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim’s system. This joint Cybersecurity Advisory identifies commonly exploited controls and practices and includes best practices to mitigate the issues. This advisory was coauthored by the cybersecurity authorities of the United States, Canada, New Zealand, the Netherlands, and the United Kingdom.

TECHNICAL DETAILS

Malicious actors commonly use the following techniques to gain initial access to victim networks.[TA0001]

- Exploit Public-Facing Application [T1190]
- External Remote Services [T1133]
- Phishing [T1566]
- Trusted Relationship [T1199]
- Valid Accounts [T1078]

Malicious cyber actors often exploit the following common weak security controls, poor configurations, and poor security practices to employ the initial access techniques.

- **Multifactor authentication (MFA) is not enforced.** MFA, particularly for remote desktop access, can help prevent account takeovers. With Remote Desktop Protocol (RDP) as one of the most common infection vector for ransomware, MFA is a critical tool in mitigating malicious cyber activity. Do not exclude any user, particularly administrators, from an MFA requirement.
- **Incorrectly applied privileges or permissions and errors within access control lists.** These mistakes **can** prevent the enforcement of access control rules and could allow unauthorized users or system processes to be granted access to objects.
- **Software is not up to date.** Unpatched software may allow an attacker to exploit publicly known vulnerabilities to gain access to sensitive information, launch a denial-of-service attack, or take control of a system. This is one of the most commonly found poor security practices.
- **Use of vendor-supplied default configurations or default login usernames and passwords.** Many software and hardware products come “out of the box” with overly permissive factory-default configurations intended to make the products user-friendly and reduce the troubleshooting time for customer service. However, leaving these factory default configurations enabled after installation may provide avenues for an attacker to exploit. Network devices are also often pre-configured with default administrator usernames and passwords to simplify setup. These default credentials are not secure—they may be physically labeled on the device or even readily available on the internet. Leaving these credentials unchanged creates opportunities for malicious activity, including gaining unauthorized access to information and installing malicious software. Network defenders should also be aware that the same considerations apply for extra software options, which may come with preconfigured default settings.
- **Remote services, such as a virtual private network (VPN), lack sufficient controls to prevent unauthorized access.** During recent years, malicious threat actors have been observed targeting remote services. Network defenders can reduce the risk of remote service compromise by adding access control mechanisms, such as enforcing MFA, implementing a boundary firewall in front of a VPN, and leveraging intrusion detection system/intrusion prevention system sensors to detect anomalous network activity.
- **Strong password policies are not implemented.** Malicious cyber actors can use a myriad of methods to exploit weak, leaked, or compromised passwords and gain

unauthorized access to a victim system. Malicious cyber actors have used this technique in various nefarious acts and prominently in attacks targeting RDP.

- **Cloud services are unprotected.** Misconfigured cloud services are common targets for cyber actors. Poor configurations can allow for sensitive data theft and even crypto-jacking.
- **Open ports and misconfigured services are exposed to the internet.** This is one of the most common vulnerability findings. Cyber actors use scanning tools to detect open ports and often use them as an initial attack vector. Successful compromise of a service on a host could enable malicious cyber actors to gain initial access and use other tactics and procedures to compromise exposed and vulnerable entities. RDP, Server Message Block (SMB), Telnet, and NetBIOS are high-risk services.
- **Failure to detect or block phishing attempts.** Cyber actors send emails with malicious macros—primarily in Microsoft Word documents or Excel files—to infect computer systems. Initial infection can occur in a variety of ways, such as when a user opens or clicks a malicious download link, PDF, or macro-enabled Microsoft Word document included in phishing emails.
- **Poor endpoint detection and response.** Cyber actors use obfuscated malicious scripts and PowerShell attacks to bypass endpoint security controls and launch attacks on target devices. These techniques can be difficult to detect and protect against.

MITIGATIONS

Applying the following practices can help organizations strengthen their network defenses against common exploited weak security controls and practices.

Control Access

- **Adopt a zero-trust security model** that eliminates implicit trust in any one element, node, or service, and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.[9],[10] Zero-trust architecture enables granular privilege access management and can allow users to be assigned only the rights required to perform their assigned tasks.
- **Limit the ability of a local administrator account** to log in from a remote session (e.g., deny access to this computer from the network) and prevent access via an RDP session. Additionally, use dedicated administrative workstations for privileged user sessions to help limit exposure to all the threats associated with device or user compromise.
- **Control who has access to your data and services.** Give personnel access only to the data, rights, and systems they need to perform their job. This role-based access control, also known as the principle of least priviledge, should apply to both accounts and physical access. If a malicious cyber actor gains access, access control can limit the actions malicious actors can take and can reduce the impact of misconfigurations and user errors. Network defenders should also use this role-based access control to limit the access of service, machine, and functional accounts, as well as the use of management privileges, to what is necessary. Consider the following when implementing access control models:

    - **Ensure that access to data and services is specifically tailored to each user,** with each employee having their own user account.
    - **Give employees access only to the resources needed** to perform their tasks.
    - **Change default passwords** of equipment and systems upon installation or commissioning.
    - **Ensure there are processes in place for the entry, exit, and internal movement of employees.** Delete unused accounts, and immediately remove access to data and systems from accounts of exiting employees who no longer require access. Deactivate service accounts, and activate them only when maintenance is performed.[11]
- **Harden conditional access policies.** Review and optimize VPN and access control rules to manage how users connect to the network and cloud services.
- **Verify that all machines, including cloud-based virtual machine instances do not have open RDP ports.** Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.[12]

Implement Credential Hardening

- **Implement MFA.** In particular, apply MFA on all VPN connections, external-facing services, and privileged accounts. Require phishing-resistant MFA (such as security keys or PIV cards) for critical services. Where MFA is not implemented, enforce a strong password policy alongside other attribute-based information, such as device information, time of access, user history, and geolocation data. See NSA's Cybersecurity Information on Selecting Secure Multi-factor Authentication Solutions, the National Institute for Standards and Technology (NIST) Special Publication 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management, and CCCS's Information Technology Security Guidance – User Authentication Guidance for Information Technology Systems for additional steps to take to enable in-depth authentication security.
- **Change or disable vendor-supplied default usernames and passwords.** Enforce the use of strong passwords. (See guidance from NIST.)
- **Set up monitoring to detect the use of compromised credentials on your systems.** Implement controls to prevent the use of compromised or weak passwords on your network.

Establish Centralized Log Management

- **Ensure that each application and system generates sufficient log information.** Log files play a key role in detecting attacks and dealing with incidents. By implementing robust log collection and retention, organizations are able to have sufficient information to investigate incidents and detect threat actor behavior. Consider the following when implementing log collection and retention:
    - **Determine which log files are required.** These files can pertain to system logging, network logging, application logging, and cloud logging.
    - **Set up alerts where necessary.** These should include notifications of suspicious login attempts based on an analysis of log files.

    - **Ensure that your systems store log files in a usable file format,** and that the recorded timestamps are accurate and set to the correct time zone.
    - **Forward logs off local systems to a centralized repository or security information and event management (SIEM) tools.** Robustly protect SIEM tools with strong account and architectural safeguards.
    - **Make a decision regarding the retention period of log files.** If you keep log files for a long time, you can refer to them to determine facts long after incidents occur. On the other hand, log files may contain privacy-sensitive information and take up storage space. Limit access to log files and store them in a separate network segment. An incident investigation will be nearly impossible if attackers have been able to modify or delete the logfiles.[13]

Employ Antivirus Programs

- **Deploy an anti-malware solution** on workstations to prevent spyware, adware, and malware as part of the operating system security baseline.
- **Monitor antivirus scan results on a routine basis.**

Employ Detection Tools and Search for Vulnerabilities

- **Implement endpoint and detection response tools.** These tools allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.
- **Employ an intrusion detection system or intrusion prevention system** to protect network and on-premises devices from malicious activity. Use signatures to help detect malicious network activity associated with known threat activity.
- **Conduct penetration testing to identify misconfigurations.** See the Additional Resources section below for more information about CISA's free cyber hygiene services, including remote penetration testing.
- **Conduct vulnerability scanning to detect and address application vulnerabilities.**
- **Use cloud service provider tools to detect overshared cloud storage and monitor for abnormal accesses.**

Maintain Rigorous Configuration Management Programs

- **Always operate services exposed on internet-accessible hosts with secure configurations.** Never enable external access without compensating controls such as boundary firewalls and segmentation from other more secure and internal hosts like domain controllers. Continuously assess the business and mission need of internet-facing services. Follow best practices for security configurations, especially blocking macros in documents from the internet.[14]

Initiate a Software and Patch Management Program

- **Implement asset and patch management processes** to keep software up to date. Identify and mitigate unsupported, end-of-life, and unpatched software and firmware by performing vulnerability scanning and patching activities. Prioritize patching known exploited vulnerabilities.

Additional Resources

- NCSC-UK Guidance – Phishing Attacks: Defending Your Organisation
- Open Web Application Security Project (OWASP) Proactive Controls: Enforce Access Controls

CONTACT

U.S. organizations: To report incidents and anomalous activity or to request incident response resources or technical assistance related to these threats, contact CISA at report@cisa.gov. To report computer intrusion or cybercrime activity related to information found in this advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch at 855-292-3937 or by email at CyWatch@fbi.gov. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

Canadian organizations: report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand organizations: report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

The Netherlands organizations: report incidents to cert@ncsc.nl.

United Kingdom organizations: report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

HOW YOU CAN HELP PROTECT CALIFORNIA

State, local, and tribal governments, non-governmental organizations and the private sector can partner with the Cal-CSIC by registering to receive Alerts and Advisories, sharing IOCs and cyber incident reports, and connecting to the California Automated Indicator Exchange.

- Email the Cal-CSIC to learn more about sharing of IOCs and connecting to the California Automated Indicator Exchange at calcsic@caloes.ca.gov.

- Report cyber incidents to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report suspicious activities or breaches of security to the Coast Guard's National Response Center (NRC), or **cyber-attacks** to the National Cybersecurity and Communications Integration Center (NCCIC):

- (NRC) Phone 1-800-424-8802 or direct phone line at 202-372-2428
- (NRC) Fax 202-372-2920
- (NRC) Web: http://www.nrc.uscg.mil/
- (NCCIC) at 888-282-0870

After calling the NRC/NCCIC, call the Captain of the Port, San Francisco, at 415-399-3530.

Other agencies you may want to consider reporting to are:

California Cybersecurity Integration Center – (916) 636-2997 and CalCSIC@caloes.ca.gov

The Federal Bureau of Investigation (FBI) should be notified of cyber security breaches:

- FBI Headquarters – threats and crime reporting: https://tips.fbi.gov/
- San Francisco Office – 415-553-7400 (san.francisco@ic.fbi.gov)
- Sacramento Office – 916-841-9110 (http://www.fbi.gov/sacramento)
- Internet Crime Center – http://www.ic3.gov/complaint/default.aspx
- InfraGard Website – https://www.infragard.org/

U.S. COAST GUARD HOMEPORT PORTAL

The U.S. Coast Guard maintains links to various sources of maritime security information on its HOMEPORT information portal. The link to U.S. Coast Guard's HOMEPORT maritime security information portal is:

- Web – http://www.homeport.uscg.mil/

CUSTOMER FEEDBACK

How are we doing? Please send feedback about this newsletter to Mr. Paul Martin, USCG Sector San Francisco, at:

- E-mail – Paul.R.Martin@uscg.mil

Note: articles appearing in this newsletter were submitted by port stakeholders or downloaded from public websites and posted without editing. If you have an article to post, please provide the article to Mr. Martin at the above e-mail address. This newsletter is a quarterly publication and generally published shortly before a meeting of the Northern California Area Maritime Security Committee. **This newsletter is for public information purposes only**; articles containing proprietary, sensitive but unclassified, or classified information will not be accepted. The U.S. Coast Guard reserves the right to decide which articles are published in this newsletter.