TLP:CLEAR

U.S. COAST GUARD

MARITIME CYBER BULLETIN

11 September 2024

MCB 03-24: Spoofed Business Websites

THREAT SUMMARY

Companies in the Shipping and Transportation sectors of the Marine Transportation System (MTS) are experiencing domain spoofing, affecting some of their customers. These fraudulent websites appear to have legitimate booking and financial transaction capabilities. It is believed that these sites aim to steal information or install malware on customers' devices. Although these spoofed websites do not directly target maritime organizations, they function similarly to watering-hole attacks, where the primary targets are the individuals and entities visiting the site.

Recommendations

The Coast Guard advises maritime stakeholders to regularly review their online presence and validate domain certificates for their legitimate websites to prevent spoofing. The validity of websites can be checked by looking up the website's registration details (such as the registrant, location, dates, history, and record information) using services like:

- ICANN (https://lookup.icann.org/)
- WHOIS (https://whois.domaintools.com/)

Maritime stakeholders who encounter fraudulent or spoofed websites should immediately inform their customers and stakeholders about these illegitimate pages and report the incident to the National Response Center. Additionally, they can use other resources to combat these malicious actors, including the FBI's Internet Crime Complaint Center (https://www.ic3.gov/), their web browser's reporting mechanism, their Internet Service Provider, and local law enforcement.

Sources

Maritime Cyber Alert 01-22 Spoofed Business Websites, https://www.dco.uscg.mil/Portals/9/Maritime%20Cyber%20Alert%2001-22%20TLP%20WHITE.pdf

Protect Your Website, CISA, https://www.cisa.gov/topics/election-security/protect-your-website

Resources

Facilities that observe any unusual activity or interruptions to their network should report those activities per Navigation and Vessel Inspection Circular (NVIC) 02-24 to:

Coast Guard's National Response Center

1-800-424-8802

OR

Cybersecurity and Infrastructure Security Agency (CISA) Central

1-888-282-0870

If you have any questions, please visit our website at: https://www.uscg.mil/MaritimeCyber or reach out to MCRB at: maritimecyber@uscg.mil

The information contained in this bulletin is provided for informational purposes only. This information is based on common standards and best practices, 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. Information Sharing Protocol: (https://www.us-cert.gov/tlp)