US Coast Guard Cyber Command
Maritime Cyber Alert 01-22

March, 25 2022

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

SPOOFED BUSINESS WEBSITES

Summary:

The U.S. Coast Guard has observed a recent uptick in malicious actors using spoofed business websites to target the Marine Transportation System (MTS). Multiple MTS partners have discovered well-constructed, fake websites masquerading as their legitimate business websites. These sites are created presumably to steal information from or install malware on customers' devices interacting with the sites.

These spoofed websites are not designed to impact the maritime organization directly but resemble watering-hole style attacks where the intended targets are individuals and entities visiting the site. The spoofed websites are professional in appearance and quite sophisticated, some of which are presenting as .com domains. This level of detail can make it difficult to discern a real site from a fraudulent one.

Mitigation:

The Coast Guard encourages maritime stakeholders whose websites could be spoofed to regularly review their online presence and validate their legitimate websites. Website authenticity can be investigated by searching the website's registration information (registrant, location, dates, history, and record information) through services such as ICANN (https://lookup.icann.org/) or WHOIS (https://whois.domaintools.com/).

Maritime stakeholders who discover fraudulent or spoofed websites should immediately notify their customers and stakeholders of the illegitimate pages and report it to their local Coast Guard unit. Maritime stakeholders may also consider utilizing other resources available 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.

While not all attacks can be prevented, the impacts can be mitigated. To avoid falling victim to a spoofed website, the Coast Guard recommends maritime stakeholders:

- **Be wary of untrusted traffic-** Treat all traffic transiting your network – especially third-party traffic – as untrusted until it is validated as being legitimate.
- **Avoid clicking on links from third parties**- Where possible, enter the correct address of the respective website manually in your browser or open it via your bookmarks.
- **Utilize a Secure Web Gateway (SWG)** - A SWG is a solution that filters unwanted software/malware from user-initiated web/internet traffic and enforces corporate and regulatory policy compliance. SWG's have many benefits including URL filtering, malicious-code detection and filtering, and application controls for popular web-based applications.
- **Keep systems updated** - Keep all hardware and software up-to-date with the latest security updates and patches.
- **Enable Multi-factor Authentication (MFA)** - Enable MFA across all applicable end-points to reduce the impacts of stolen user credentials during a successful attack.

Resources:

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

As a reminder, further information on cyber threats, vulnerabilities, and guidance is available at CISA's Shields Up website (https://www.cisa.gov/shields-up). Stakeholders should continually monitor this site, in addition to Coast Guard messaging, for important updates.