From: John Jorgensen
Sent: Wednesday, August 24, 2016 11:08 AM
Subject: Maritime SIG announcements [IMPORTANT]

Members, our next meeting will be on [[Thursday 15 Sep]], and I'll send additional information as we get closer to the date.

In the meantime, we have some information that is of immediate interest.

1- A particular flaw in a transportation logistics application was publicized this morning. This is from FireEye this morning:

"Attackers Exploit Flaw in Software Used by US Ports

From The Media

An SQL injection vulnerability was discovered in a transportation logistics application used worldwide. Navis WebAccess provides transport operators real-time access to logistics information. The application's publicly accessible news pages reportedly contain an SQL injection vulnerability (CVE-2016-5817) that can allow an attacker to remotely modify or read data. According to US-CERT, affected organizations received a patch; however, several US-based organizations were successfully attacked and experienced data loss. Read the Story: Security Week

Analyst Comment

We judge that exploitation of CVE-2016-5817 poses a serious threat to organizations using affected Navis software, as attackers are reportedly exploiting this vulnerability in the wild. This could allow attackers to read or modify contents of the application's SQL database. The publicly available proof-of-concept code makes it easier for additional actors to develop functional exploit code. While Navis has reportedly distributed custom patches to affected organizations, it is uncertain how many organizations have applied the patches, potentially leaving a sizable set of targets for attackers."

The Security Week article (http://www.securityweek.com/attackers-exploit-flaw-software-used-us-ports) cites Port of Houston Authority as a user of this software, among others. I would encourage anyone with connection to local ports (Houston, Galveston, Corpus, Texas City, etc.) to read the article, the related post on ICS-CERT, and understand the potential risk conditions you may encounter.

2- From US-CERT this morning, a warning about scams relating to the recent floods in LA:

"FTC Releases Alert on Louisiana Flood Disaster Scams

08/23/2016 07:48 PM EDT

Original release date: August 23, 2016

The Federal Trade Commission (FTC) has released an alert on scams that cite the recent flood disaster in Louisiana. These charity scams take many forms, including emails containing links or attachments that direct users to phishing or malware-infected websites. Donation requests from fraudulent charitable organizations commonly appear after major natural disasters.

US-CERT encourages users to take the following measures to protect themselves:

- Review the FTC alert and its information on Charity Scams.
- Do not follow unsolicited web links or attachments in email messages.
- Keep antivirus and other computer software up-to-date.
- Check this Better Business Bureau (BBB) list for helping Louisiana flood victims before making any donations to this cause.
- Verify the legitimacy of any email solicitation by contacting the organization directly through a trusted contact number. You can find trusted contact information for many charities on the BBB National Charity Report Index.
- Refer to Security Tip ST04-014 – Avoiding Social Engineering and Phishing Attacks – for more information on social engineering attacks."

More at (https://www.us-cert.gov/ncas/current-activity/2016/08/23/FTC-Releases-Alert-Louisiana-Flood-Disaster-Scams)

3- The Houston InfraGard chapter meeting will be Wednesday, 21 Sep, 1200-1500.

Date & Time: Wednesday, September 21, 2016, 12:00 - 3:00 pm

Lunch Sponsor: Carrier 1 Data Centers

Venue: Harris County Department of Education Conference Center

Address: 6300 Irvington Blvd., Houston, TX 77022

Topic: Phishing, E-Fraud & The Darknet

4- Two recent reports may be of interest to you, released from DHS within the last month. They are attached.

5- A Maritime Information Sharing and Analysis Organization (ISAO) has stood up in FL. SA Angela Haun and I meet with a representative today at ABS HQ to see how we can bring effectively interface with the new organization and build mutually-beneficial information flows. More on this at the next meeting.

6- The "Ransomware Roadshow" will be held on Thursday 22 Sep.

NEW! You are also invited to attend the **Ransomware 101 Workshop on Thursday, September 22, 2016 from 8:30 am – 12:15 pm** at Marriott West Loop South. The FBI, USSS, Financial Services ISAC, Multi-State ISAC, National Health ISAC, Palo Alto Networks and Symantec will be sharing their experiences and expertise around ransomware, why you should be concerned and how you can protect against becoming the next victim. (Please pardon the typo in the attached flyer.) There is no cost to attend this half-day workshop, where experts in cybersecurity will:

- Describe ransomware;
- Cover the tactics, techniques and procedures used by the criminals;
- Provide the threat landscape;
- Discuss why situational awareness and information sharing are important;
- Offer strategies to help protect your organization from ransomware attacks.

**** TO REGISTER GO TO HTTPS://WWW.REGONLINE.COM/RANSOMWAREROADSHOW ****

7- US-CERT also passed good information about mitigating malicious email.

"ACSC Releases Risk Mitigation Strategies Against Malicious Email

08/01/2016 05:13 PM EDT

Original release date: August 01, 2016

The Australian Cyber Security Centre (ACSC) has published guidance to organizations on risks posed by malicious email. Systems infected through targeted email phishing campaigns act as an entry point for attackers to spread throughout an organization's entire enterprise, steal sensitive business or personal information, or disrupt business operations.

US-CERT encourages users and administrators to review the ACSC publication on Malicious Email Mitigation Strategies and US-CERT Alert TA15-213A for additional information."

See ACSC's page for more info (http://asd.gov.au/publications/protect/malicious_email_mitigation.htm).

8- The next meeting of the Ship Operators Collaborative Program (SOCP) will be in Houston at the Greenspoint Conference Center, right next to ABS HQ and across the street from the Greenspoint Mall, 5-6 Oct. SOCP works with mariners, facility owners and regulators (i.e., USCG) for mariner training and licensing, compliance issues, skill-building, and safety improvement programs. This semi-annual meeting will center on best practices, cybersecurity and safety afloat and ashore. If you'd like more information, please contact me. I'll have information at the 15 September meeting, also.

I'll send the initial announcement for our next stated meeting within the next few days. Please pass this announcement along to anyone who may have interest in our SIG and the maritime community.

John M. Jorgensen, CISSP-ISSAP
Director, Cybersecurity and Software
American Bureau of Shipping

16855 Northchase Dr.
Houston, TX 77060-6008
USA
281-877-6675 (office)
832-707-6165 (cell)
JohnJorgensen@eagle.org
www.eagle.org