NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
January 2015 (Edition 2015-1)

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 news letter will be e-mailed to members of the Northern California Area Maritime Security Committee, posted on the Coast Guard's HOMEPORT portal and may be posted by the San Francisco Marine Exchange.

TABLE OF CONTENTS

Content	Page
• Article Summaries	1
• Cyber Security	2
• Ransomware Malware in the MTS	3
• Cyber Crime and the Shipping Industry (Article Summary)	4
• Big Data Is Stopping Maritime Pirates ... From Space	4
• Maritime Cybersecurity: A Growing Threat Goes Unanswered (Article Summary)	6
• Maritime Cyber Risks (Article Summary)	6
• Unwitting Workers Give Hackers Keys to Fortune 500 Firms' Networks: Study	7
• Keeping Our Critical Infrastructure Cyber-Secure	8
• Identifying Cyber Vulnerabilities	9
• USTRANSCOM Contractors Vulnerable to Cyber Targeting	10
• USCG Announcement – Cyber Security Public Meeting	10
• Lesson Learned – Port of Stockton	11
• Cyber Incident Report Phone Numbers	13

ARTICLE SUMMARIES

- **Cyber Security** – discusses measures that port stakeholders can take to harden their computer systems.
- **Ransomware Malware in the MTS** – discusses what it is and how criminals have used false "DHS banners" to gain access to computer systems.
- **Cyber Crime and the Shipping Industry** (Article Summary) – discusses various methods criminals use to use industry computer systems for their activities. This lengthy article is an attached document.

- **Big Data Is Stopping Maritime Pirates ... From Space** – discusses how data monitoring can detect cyber-crimes and activities.
- **Maritime Cybersecurity: A Growing Threat Goes Unanswered** (Article Summary) – discusses two government reports highlighting cyber-security vulnerabilities. This lengthy article is an attached document.
- **Maritime Cyber Risks** (Article Summary) – discusses a wide range of cyber-security issues and risks. This lengthy article is an attached document.
- **Unwitting Workers Give Hackers Keys to Fortune 500 Firms' Networks: Study** – discusses how company workers unwittingly create cyber-attack vulnerabilities of their businesses' computer systems.
- **Keeping Our Critical Infrastructure Cyber-Secure** – discusses how persons can keep their computer secure through good cyber security "hygiene".
- **Identifying Cyber Vulnerabilities** – discusses DHS efforts in combating cyber-crimes and how you can report them.
- **USTRANSCOM Contractors Vulnerable to Cyber Targeting** – is an FBI Private Industry Notification (PIN) highlights foreign cyber actors targeting Department of Defense (DoD) maritime contractors; it is attached to the end of this newsletter.

MAIN ARTICLES

USCG (10/31/2014), Cyber Security – written by David E. Sanger, David Barboza and Nicole Pelroth

American ports, terminals, ships, refineries, and support systems are vital components of our nation’s critical infrastructure, national security, and economy. Cyber-attacks on industrial control systems could kill or injure workers, damage equipment, expose the public and the environment to harmful pollutants, and lead to extensive economic damage. The loss of ship and cargo scheduling systems could substantially slow cargo operations in ports, leading to backups across the transportation system. A less overt cyber-attack could facilitate the smuggling of people, weapons of mass destruction, or other contraband into the country.

In short, there are as many potential avenues for cyber damage in the maritime sector as there are cyber systems. While only some cyber-attack scenarios in the maritime sector could credibly lead to a Transportation Security Incident, we must identify and prioritize those risks, take this threat seriously, and work together to improve our defenses.

Fortunately, the men and women of the United States Coast Guard take our responsibility to protect the nation from threats seriously. As in other areas, we will work with the private sector, and with other federal, tribal, state, and local agencies to address this new threat. The President’s recently signed cyber security Executive Order sets requirements for executive branch agencies to address cyber risks. We have started that work already, and will keep the private sector informed of our progress. We will also be asking for advice and cooperation.

What can be done:

Fortunately, the process for doing so is parallel in structure to that of other security and safety efforts: assess risk, adopt measures to reduce that risk, assess progress, revise, and continue. These processes, taken together, can significantly improve an organization's risk reduction efforts and increase resilience through continuity of business planning.

Looking specifically at cyber security, consider the following steps:

- Conduct a Risk Assessment – begin by assessing what parts of your enterprise are controlled or supported by computer systems. What are the consequences should those systems become inoperable, controlled by outside parties, or misused by internal parties?
- Identify and Adopt Best Practices – what information technology security standards are most applicable to your systems? Are your systems meeting those standards, are your employees familiar with them? When were they last updated? What backup systems, redundancies, or replacements are available?
- Secure Your Supply Chain – As with just-in-time inventory and production systems, consider the cyber vulnerabilities and practices of your suppliers, customers, and other organizations critical to your company's profitability. Discuss cyber security with those organizations and consider incorporating good cyber practices into marketing and contracting.
- Measure Your Progress – Test your cyber practices through drills and exercises. Identify any gaps or lessons learned, and set specific goals with timelines for making needed improvements.
- Revise and improve security – Review your latest risk assessment, evaluate any new cyber systems you may have added since that time, incorporate lessons learned and revise your cyber security policies and procedures accordingly.
- One way to start this process is to take advantage of the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICSCERT). ICS-CERT provides a wide range of information, tools, and services that can help companies assess their security, identify recommended practices, and improve their cyber security. http://ics-cert.us-cert.gov/

USCG (10/31/2014) Ransomware Malware in the MTS (USCG HOMEPORT article)

DHS and the Coast Guard have received reports of increased activity concerning ransomware malware infection occurring throughout the world. Recently, a maritime facility fell victim to a ransomware malware infection. Malware such as this could have a detrimental effect on the facility's business and production systems. Users that are targeted by the ransomware receive a message claiming that the use of their computer has been suspended and that the user must pay a fine to unblock it.

One iteration of this malware falsely claims to be from DHS and displays a DHS-themed banner that makes it appear legitimate. Ransomware is not easily detected by security software, but if an attack is suspected in its early stages, immediate removal of the malware can limit the damage to the data. Users that are infected with the malware should consult with a reputable security expert to assist in removing the malware. DHS and the Coast Guard encourage users and administrators to NOT pay the perpetrators.

Use caution when encountering these types of email messages and take the following preventative measures to protect yourself from phishing scams and malware campaigns that attempt to frighten and deceive a recipient for the purposes of illegal gain:

- Do not follow unsolicited web links in email messages
- Use caution when opening email attachments. Refer to the Security Tip Using caution with Email Attachments for more information on safely handling email attachments.
- Maintain up-to-date antivirus software.
- Users who are infected should change all passwords AFTER removing the malware from their system.
- Refer to the Recognizing and Avoiding Email Scams (pdf) document for more information on avoiding email scams.
- Refer to the Security Tip Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

If you're the victim of ransomware malware or any cyber event, we request you report this incident, along with any other suspicious activity, to the National Response Center at 1-800-424-8802, in accordance with 33 CFR 101.305. Victims are also encouraged to report the incident to the FBI at the Internet Crime Complaint Center (IC3).

FBI (11/03/2014) Cyber Crime and the Shipping Industry, By Colum Bancroft (Article Summary)

With the international shipping industry estimated to carry over 90 percent of today's world trade, the temptation for criminals has never been greater. Savvy criminals around the globe are exploiting cyber vulnerabilities to perpetrate a wide range of crimes — from longstanding physical ship-related dangers like piracy and smuggling to more recent financial-related frauds like the diversion of payments. The challenge for ship owners is even more complex because cyber criminals are targeting diverse facets of the shipping industry. For example, there was a well-documented case of drug smugglers subverting an IT system at a major port in order to facilitate the smuggling of contraband in containers... (**For the rest of the seven page article, see the attachment at the end of the newsletter**).

Forbes Magazine (11/11/2014) Big Data Is Stopping Maritime Pirates ... From Space

Somali pirates, made famous in a recent Tom Hanks film, are the scourge of the oceans. Maritime pirates typically board a commercial tanker and disable the Automatic Identification

System (AIS) tracking system, causing the boat to “disappear” for several days. But a new company says it can keep track of these floating assets, despite the pirates.

Spire is a San Francisco-based global startup with offices in Singapore that is in the business of launching into Low Earth Orbit a constellation of shoebox-sized satellites. Right now Spire focuses on covering the 75 percent of the earth that doesn’t have satellite coverage—namely the maritime areas.

Speaking at the RE: WORK Internet of Things Summit in San Francisco, Chris Wake, head of business operations, said his company: “listens where others only see.” In particular, he said “The primary technologies that we have onboard today relate to radio signal processing and remote sensing. In particular, for maritime domain awareness, we capture and process AIS vessel tracking data, and for terrestrial weather data we use a technology called GPS radio occultation.” Piracy, Wake said, most often occurs along the coasts of Africa. However, piracy is a global phenomenon. According to European Union's Navfor; there is a $6 billion per annum impact to the world’s economy as a result.

When a pirate seizes a ship, Wake said in a follow-up email to Forbes.com, “Our software looks for anomalies (e.g. missing signals), and [our satellites have] other sensors onboard to validate or invalidate what is happening with those ‘vanishing’ ships.” Spire’s satellites sweep the earth hourly, so the information is timely and actionable.

Placing Spire’s satellites over the world’s oceans also benefits a number of very different industries, from maritime insurance to financial services to global trade monitoring, to search and rescue, he said. In addition to tracking commercial ships, Spire could also one day provide telemetry on commercial jets.

Why even go into the nano-satellite business? Two reasons, Wake said. One, government-sponsored satellites are old and falling out of the sky. And they are not being replaced. US Government agencies are increasingly looking to private enterprises to fill the void. Although commercial rockets have not fared well this month, Wake said his company isn’t concerned. They expect to lose a few nano-satellites along the way, he said. Two, traditional commercial satellites, such as those in geostationary orbit, are very large and were designed to last for many years. Problem is, says Mr. Wake; we live in a world defined by Moore’s law which states that the number of transistors on a circuit doubles every two years. So Spire uses the cellular phone model in that it replaces its satellites every eighteen months to two years. This allows the company to update its technology more frequently.

The form factor used by Spire is the standard Cube-Sat design, usually a 10 cm cube. The company uses off-the-shelf, low cost production and a four-month design to delivery lifecycle.

They can deploy many nano-satellites in one rocket launch at a fraction of the traditional cost. Companies and governments, however, do not buy the individual satellites from Spire. Instead they buy access to the "fire hose" of data from Spire, Wake said, referring to Twitter's famous blog. At the moment Spire produces only raw data, but the company hopes to one day also provide some analytics as well. Governments have been very interested in Spire's data. Wake said that developing countries are keen on knowing about illegal fishing in their offshore waters. "This is a big deal."

This article is available online at: http://onforb.es/1szw4Xh 2014 Forbes.com LLC™ All Rights Reserved. Online news article; Forbes; www.forbes.com; 11 November 2014; "Big Data Is Stopping Maritime Pirates ... From Space"; http://www.forbes.com/sites/robertvamos/2014/11/11/big-data-is-stopping-maritime-pirates-from-space/2/

FBI (10/22/2014) Maritime Cybersecurity: A Growing Threat Goes Unanswered, By Steven L. Caponi and Kate B. Belmont (Article Summary)

Reports issued by the United States Accountability Office ("GAO") and the European Network and Information Security Agency ("ENISA") confirm that the maritime industry is as susceptible to cybersecurity risks as the most cutting-edge technology firms in Silicon Valley. With the ability to commandeer a ship, shut down a port or terminal, disclose highly confidential pricing documents, or alter manifests or container numbers, even a minor cyber attack can result in millions of dollars of lost business and third-party liability... This article discusses issues raised by both reports. (**For the rest of the three page article, see the attachment at the end of the newsletter**).

FBI (10/15/2014) Maritime Cyber Risks, CyberKeel, Copenhagen, Denmark (Article Summary)

When the term "cyber risk" is mentioned, this typically invokes one of three different mental associations with most people. Either it signals that this is a highly technical area on which they have little or no influence, or that this is the realm of writers of action movies featuring geeky characters or finally that this is something which only happens to someone else. This behavior is replicated for the majority of business industries, including the maritime sector. The three typical reactions mentioned all lead towards the same behavior. Most people get to the conclusion that cyber security is the responsibility of the IT department, and apart from that there is nothing they can really do. Unfortunately this has a direct, and negative, impact. Certainly some aspects of cyber security require technical knowledge and skill, but need to be seen in the context of several other aspects which tend to be non-technical in nature. First of all, management need to be involved in making decisions pertaining to the level of security a company wants, as very often increased levels of cyber security comes at the price of having to modify business processes in such a way that daily business operations might be impacted. It is then a clear strategic risk decision which has to be made, and not a specific IT decision. Secondly, the most vulnerable attack point related to cyber security is people. Hacking into company systems using only your computer from afar, whilst possible, is often quite difficult if the company has good cyber defense systems. However, getting employees to do things online, which they should not do, or attacking the employee's smart-phones while they are at conferences, or getting physical access to an office and installing your own devices into employee computers, is much easier. (**For the rest of the twenty-six page article, see the attachment at the end of the newsletter**).

CNN (10/29/2014), Unwitting Workers Give Hackers Keys to Fortune 500 Firms' Networks: Study – By Mike Brunker (First published October 29 2014, 5:00 AM)

Forty-four percent of Fortune 500 companies have had their employees' stolen email addresses and passwords exposed in Internet forums used by hackers this year, giving criminals potential entrée to customer data and critical U.S. infrastructure, according to a new report. The data firm Recorded Future scoured Internet forums and "paste sites" – web applications typically used to share computer code -- from Jan. 1 through Oct. 8 to uncover the vulnerability involving employee "credentials" – the combination of an email address and password. Recorded Future found that 221 of the nation's top companies had employee credentials exposed, including 51 percent of the leading financial firms, 62 percent of technology firms and 49 percent of public utilities.

"The presence of these credentials on the open web leaves these Fortune 500 companies vulnerable to corporate espionage, socially engineered cyber-attacks and tailored spear-phishing attacks," the report said. The employees also put themselves at risk on any services with which they may have used the same email and password combination, such as online banking. The exposure of public utilities' security practices were particularly concerning, because hackers could conceivably gain control of parts of the electrical grid or dams. Recorded Future research highlighted "multiple public utilities with webmail logon pages easily discovered with Google searches."

Most of the exposures occurred through third-party websites. Employees often registered on the sites using their work email accounts to engage in seemingly innocuous activities such as posting commentary on blogs, reviewing hotels or restaurants or participating on hobbyist websites, it said. Many of these smaller sites lack sophisticated security and are susceptible to hackers, said Scott Donnelly, who conducted the analysis for Recorded Future. While most such sites encrypt or "hash" passwords to avoid revealing them in plain text, such protections are often easily overwhelmed using modern hacking tools that are "open-source and readily available," he said.

“At that point it becomes a coin flip … whether or not that‘s a valid log-on for that company account as well,” Donnelly told NBC News, referring to numerous studies showing that computer users frequently reuse passwords so they can remember them.

Compounding the problem is the fact that security breaches on smaller sites are rarely reported to authorities, meaning that the employees and corporate IT managers are often unaware that the information has been exposed, said Christopher Ahlberg, Recorded Future’s founder and CEO. “You’re not going to see a CNET.com story if it’s a neighborhood 5k run that gets hacked,” he said.

The report did not attempt to quantify how often stolen credentials were used to launch cyber-attacks against the Fortune 500 companies. But it cited a recent claim by hackers who said they stole 7 million user names and passwords from the popular cloud storage service Drop-box as following the credential-theft model. “Attackers … used these stolen credentials to try to log into sites across the Internet, including Drop-box,” it said.

Drop-box has denied it was the source of the data breach, blaming unidentified third-party services. It is unclear what role – if any – credential theft from employees may have played in recent high-profile corporate hacks in which the cyber-attackers absconded with customer data. But Donnelly, the report’s author, said the hack of Target – itself a Fortune 500 company – was similar in that the theft began with the theft of network credentials from a subcontractor, a heating and air conditioning supplier, according to security blogger Brian Krebs. The report said so-called paste sites that allow users to store and share plain text, “have become a dumping ground for stolen credentials.” Donnelly said such information is often removed quickly by site administrators, but that even brief exposure can give hackers an opportunity to copy it, he said.

DHS (10/31/2014) Keeping Our Critical Infrastructure Cyber-Secure, October 20, 2014, Suzanne E. Spaulding, Under Secretary, NPPD

We all are increasingly reliant on the Internet. Not just when we’re on a laptop or smart phone. The underlying critical infrastructure that provides essential services to all of us also is becoming more dependent on the internet. While these cyber-dependent networks and devices offer greater convenience and efficiency, they also come with potential risks and threats to our security.

DHS recognizes that these emerging cyber threats require the engagement of our entire society – from government to the private sector and members of the public. Pursuant to the President’s Executive Order 13636: Improving Critical Infrastructure Cybersecurity, the National Institute for Standards and Technology developed and released a Cybersecurity Framework, a collection of cybersecurity standards available to critical infrastructure owners and operators and governments. To help entities implement the Framework, DHS launched the C^3 Voluntary Program. This public-private partnership assists businesses of all sizes, and at all levels, from the board room to the IT department and everyone in between, as well as government, educational institutions, and households all across the country, to become more secure online.

Consumers play an important role in helping to secure critical infrastructure not only by practicing good cyber hygiene themselves, but also by becoming well-informed about whether the companies and organizations they do business with adhere to high cybersecurity standards. On an individual basis, consumers can:

- Read the privacy policy of a company or vendor before purchasing a product or service from them.
- Beware of requests to update or confirm personal information online. Most organizations do not ask for personal information over email.
- Make sure websites that ask for personal information (e.g., to pay a utility bill) use encryption to secure their sites.
- Learn about steps to enhance security and resilience in local businesses and communities.
- By working together, we can protect the critical infrastructure on which we all we rely, keeping ourselves, our families, and our communities safer and more secure from threats both physical and cyber.

DHS (10/31/2014) Identifying Cyber Vulnerabilities, October 29, 2014

Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyber-attacks such as Corporate Security Breaches, Spear Phishing, and Social Media Fraud. Cybersecurity is a shared responsibility, and each of us has a role to play in making it safer, more secure and resilient.

Collaborating to Enhance Cyber Security

To address the evolving threats and increased risks of cyber-crimes, DHS works directly with public and private partners to enhance cybersecurity. We work to promote cybersecurity awareness and digital literacy amongst all Internet users. DHS also collaborates with the financial and other critical infrastructure sectors to improve network security. Additionally, DHS components such as the U.S. Secret Service and U.S. Immigration and Customs Enforcement (ICE), have special divisions dedicated to combating cyber-crime.

Combating Cyber Crime

The Secret Service maintains Electronic Crimes Task Forces (ECTFs), which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service's Cyber Intelligence Section has directly contributed to the arrest of transnational cyber criminals responsible for the theft of hundreds of millions of credit card numbers and the loss of approximately $600 million to financial and retail institutions. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cyber training and information to combat cyber-crime. ICE's Cyber Crimes Center (C3) works to prevent cyber-crime and solve cyber incidents. From the C3 Cyber Crime Section, ICE identifies sources for fraudulent identity and immigration documents on the Internet. C3's Child Exploitation Section investigates large-scale producers and distributors of child pornography, as well as individuals who travel abroad for the purpose of engaging in sex with minors.

Law Enforcement Cyber Incident Reporting

The Law Enforcement Cyber Incident Reporting resource provides information for State, Local, Tribal, and Territorial (SLTT) law enforcement on when, what and how to report a cyber-incident to a federal entity. The document also provides information on federally sponsored training opportunities and other useful resources available to SLTT law enforcement (**see attached flyer**).

On the Department of Homeland Security's website for cyber security there is an article discussing how to secure your web-browser. It is too long to present in this newsletter, but the following URL will take you to the article – https://www.us-cert.gov/publications/securing-your-web-browser.

FBI (11/21/2014) USTRANSCOM Contractors Vulnerable to Cyber Targeting

This Private Industry Notification (PIN) highlights foreign cyber actors targeting Department of Defense (DoD) maritime contractors and the need for timely reporting of intrusions. During a 12-month period beginning on 1 June 2012, there were approximately 50 computer intrusions or other cyber events where the networks belonging to the US Transportation Command (USTRANSCOM) maritime and aerial services contractors were targeted. The US Intelligence Community believes that at least 20 of the 50 incidents were attributed to state-sponsored actors employing *advanced persistent threat* a tactics. Yet, in some instances, USTRANSCOM remained unaware that foreign cyber actors were actively targeting its maritime contractors. There are several explanations as to why USTRANSCOM was unaware that its contractors were being targeted: a failure on the part of the contractors to report intrusions, a failure on the part of the contractors to report attempted intrusions to USTRANSCOM, and the contractor's inability to detect successful cyber-attacks or report intrusion attempts that were being dismissed as having failed, considered isolated and/or insignificant. (**For the complete text of the PIN, see the attachment at the end of the newsletter**).

USCG (12/15/2014) Cyber Security Public Meeting – Announcement

Cyber security issues are a growing risk factor within the Marine Transportation System. The Coast Guard has previously provided guidance to the maritime industry on this topic, such as the NIST Cyber Security Framework and cyber security information on Homeport. The U.S. Coast Guard is now developing policies to address MTS cyber security risks in a more consistent fashion. A Notice (found at https://www.federalregister.gov/articles/2014/12/12/2014-29205/guidance-on-maritime-cybersecurity-standards) published on December 12, 2014 announced that the U.S. Coast Guard will host a public meeting at the Department of Transportation Building in Washington D.C. on January 15, 2015 from 9:00 a.m. to 12:00 p.m. The intent of the meeting is to allow the public, including the maritime industry, to provide suggestions, comments, and concerns about how the Coast Guard should approach this policy development effort. While this is the earliest stage of this process, the Coast Guard expects to develop policies that will assist facility and vessel operators to address cyber security vulnerabilities that could cause or contribute to a Transportation Security Incident. These vessel and facility operators are regulated by the Maritime Transportation Security Act (MTSA). Please read the notice in its entirety to gain specific information on the public meeting. Seating is limited, so please reserve a seat as soon as possible, but no later than January 5, 2015. The Coast Guard will post a video recording of the meeting on the docket as soon as possible after the meeting concludes.

To reserve a seat, please email Josephine.A.Long@uscg.mil with the participants first and last name for all U.S. Citizens, and additionally official title, date of birth, country of citizenship, and passport number with expiration date for non-U.S. Citizens. To gain entrance to the Department of Transportation Headquarters building, all meeting participants must present government-issued photo identification (i.e. state issued driver's license). If a visitor does not have a photo ID, that person will not be permitted to enter the facility. All visitors and any items brought into the facility will be required to go through security screening each time they enter the building.

A live video feed of the meeting will be available upon request to Josephine.A.Long@uscg.mil. The Coast Guard will accept comments at the public meeting. The public may also submit comments to the docket as described in the Federal Register notice.

PORT STAKEHOLDER LESSON LEARNED

Port of Stockton (12/08/2014) Lesson Learned, By Port of Stockton

The day was progressing along like most days….minor support calls and systems running as they should. From an IT standpoint, all systems were in check and working well. It was Wednesday afternoon, late in the day. Then the call came in…..an end-user who was having difficulty accessing a file in their departmental shared folder. This particular file was an Excel Spreadsheet that is accessed to log information periodically. The error the user reported was that Excel showed the file was corrupt. This was followed by our typical investigation and information gathering phase. "When did you last access the file?" "When was the last time you opened and worked with the file?" The finally, "Where is the file located?"

At this point, I browsed to the location where the file was. The file was an Excel file, however, when I selected the file, the preview pane did not show the file but that there was an error in the preview. As a typical part of investigation, I will look at the details of the file to see who worked on the file last. Since this was a Windows environment, I simply clicked the file and selected properties and then details. After glancing at the details of the file, I noticed that *John Doe* had modified the file. Since he was in another department, this struck me as being abnormal. I then quickly checked a few more files in the directory and they had the same issue! Now I was really concerned. I went to *John's* department folder and checked files there; all of the Excel files were now corrupt!

MALWARE! I have seen this before with CryptoLocker. Being that we are in a Virtualized Environment, I knew we could eliminate this quickly, but first, we needed to kill the process. I called *John's* office and his Administrative Assistant informed me that he was gone for the day. That particular week, he was in and out of the office; long enough for a "drive-by corrupting"! I immediately logged into the master console for the virtualized desktops and checked to see if he had shutdown, logged out, or simply closed the client and left the machine running. Fortunately, we have tried to educate the users on shutting down the machines to give the better performance over simply leaving them running all the time. The reboot replenishes depleted system resources and give the machine new life. In this case, he had shutdown the machine prior to leaving for the day. Now that I knew his machine was not in action and happily corrupting files, I moved on to the remediation phase.

Starting with the Virtual Desktop and using the VMWare Horizon View administrative console, I recomposed John's desktop to our last updated build which is known to be good. This process would take some time, so I now dove back to the files to see when the damage took place. Being very experienced with advanced network systems and of course the importance of business continuity in regards to data backup and recovery, one of the things I have done on the fileserver is to enable VSS (Volume Shadow Copies). This technology allows for all data to have snapshots taken at scheduled times to allow a roll back to point-in-time versions of files. I have this set for every 6 hours at 6am, 12pm, 6pm, and 12am. I have found this to work very well in most environments. In addition, if an immediately available snapshot will not go back far enough, I could leverage the infrastructure backups which contain all systems backup files over a longer period of time. These backups are stored to a local disk based backup storage device which stays on-site at all time to allow quick recovery of backed up data. The jobs stored on this local backup drive are also replicated to two additional backup drives which alternate from on-site to a protected environment offsite. This insures rapid response along with offsite storage in case of a local disaster. In this case, I determined that the issue had started on Monday morning at 9:27am. I proceeded to investigate the extent of the damage. It appeared that it only affected departments who had chosen not to lockdown their network shared folder, and of course, all of John's files. The target roll back would be Monday Morning at 6:00am.

After going through and reverting files to their useable state and recomposing John's VM to a clean status, it was then time to investigate how this happened. After checking with another I.T. colleague, I was informed that John had complained Monday morning about not being able to open some of his files. This information was not discussed until after the event, which is how this made it all the way through Wednesday before detection. We have now agreed that any future file access issues or anything out of the ordinary should be discussed immediately to insure that if it is an event, we could immediately resolve the issue. What he had discussed with John on Monday was that John had clicked on an Ad he should not have prior to him losing access to his personal files. We had determined this was NOT CryptoLocker, but a copycat piece of Malware. You see, I had already locked the system down to prevent CryptoLocker from being able to infect our machines by disabling installations from occurring in the "temp" folder.

Our lessons learned from this event are; 1) to keep constant communication going between support personnel and end-users, and 2) continued education of the end-users is very important. We encourage our users to report anything out of the ordinary even if they did something they should not have done. If they keep silent on these types of events, damage will be more widespread. While maintaining a standard of best practices by keeping systems patched, firewalls up-to-date, virus signatures current, and regular multiple layers of backup are absolutely a must to provide business continuity and resiliency of information systems, communication between support staff and users is paramount.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report cyber intrusions and every other security breach to the Coast Guard's National Response Center (NRC):

- Phone 1-800-424-8802 or direct phone line at 202-372-2428
- Fax 202-372-2920
- Web: http://www.nrc.uscg.mil/

The Federal Bureau of Investigation (FBI) also wants to 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
- IngraGard 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 and posted with minimal 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.