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, posted on the Coast Guard's HOMEPORT portal and may be posted by the San Francisco Marine Exchange.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many Operators Open to Simple Cyber Attack</td>
<td>3</td>
</tr>
<tr>
<td>CCICADA Addresses the Growing Threat of Maritime Cyber-Attacks</td>
<td>5</td>
</tr>
<tr>
<td>United States: Maritime Cyber Attacks: Changing Tides and the Need for Cybersecurity Regulations</td>
<td>7</td>
</tr>
<tr>
<td>Cyber Security: The Anatomy of a Cyber Intrusion</td>
<td>9</td>
</tr>
<tr>
<td>DHL Customers Being Targeted in New Phishing Email Scam</td>
<td>13</td>
</tr>
<tr>
<td>Adware Program Vonteera Blocks Security Products with Simple Windows UAC Trick</td>
<td>14</td>
</tr>
<tr>
<td>Crafty Spear-Phishing Campaign Uses Terror Attack to Increase Proficiency</td>
<td>16</td>
</tr>
<tr>
<td>Cyber Incident Report Phone Numbers</td>
<td>17</td>
</tr>
</tbody>
</table>

ARTICLE SUMMARIES

- **Many Operators Open to Simple Cyber Attack** – Software security company CyberKeel evaluated the top 50 container carriers’ websites in 2014 and found most companies were open to simple cyber security attack.

- **CCICADA Addresses the Growing Threat of Maritime Cyber-Attacks** – Modern ships contain highly sophisticated communications and navigation systems. Seen here is a VisionMaster FT Integrated Bridge System by Sperry Marine. Fierce storms and lashing seas are no longer the greatest threats to maritime commerce. Today’s biggest threats are stealthy, invisible and almost impossible to detect. They are called “cyber-attacks,” and they can be carried out with growing ease by astute terrorists and other adversaries who have the technical know-how to take remote control of—or interfere with the operations of—large ships, ports and oil rigs.
• **United States: Maritime Cyber Attacks: Changing Tides and the Need for Cybersecurity Regulations** – cyber-attacks on government agencies and the world's largest companies have become a regular occurrence. Recent cyber-attacks reported by the mainstream media include the cyber-attack against SONY, Anthem Health Insurance, the White House, the Office of Personnel Management ("OPM"), Ashley Madison, and even the Houston Astros. As the list of companies and agencies that suffer cyber-attacks grows longer, it is clear and undeniable that no industry is safe, and any company that relies on information and communication technology ("ICT"), must take the appropriate steps to protect itself against cyber threats. Although the maritime community has not yet garnered front-page attention as a victim of a recent cyber-attack, make no mistake, the maritime industry is one of the most heavily targeted industries in the world and also suffers cyber-attacks regularly.

• **Cyber Security: The Anatomy of a Cyber Intrusion** – Compromising the cyber integrity of the network threatens every user and every system on your ship or in your building. Violating security best practices, circumventing security policies, carelessness and falling victim to social networking exploits opens the door to cyber adversaries who can exploit vulnerabilities which may directly impact our Navy's warfighting capability and potentially threaten our lives.

• **DHL Customers Being Targeted in New Phishing Email Scam** – With the holiday season fast approaching, the shipping of packages and gifts will reach a fever pitch over the next two months. This is the time when cyber criminals are looking to strike, not only stealing critical financial information, but looking for ways to steal personal information.

• **Adware Program Vonteera Blocks Security Products with Simple Windows UAC Trick** – A well-known adware program is preventing users from installing antivirus products by leveraging a Windows feature that was designed for security. The program, known as Vonteera, abuses the digital signature check performed by the Windows User Access Control (UAC) for executable files.

• **Crafty Spear-Phishing Campaign Uses Terror Attack to Increase Proficiency** – Cyber-criminals are using the fear generated from the recent wave of terror attacks to target corporate offices in the Middle East and Canada with spear-phishing attacks. One of the more sinister aspects of this campaign is the amount of obfuscation being used by the attackers, to include the names of real security officials and even some legitimate attachments.
(USCG 2015) Many Operators Open to Simple Cyber Attack (6/10/2015) By Wendy Laursen

Software security company CyberKeel evaluated the top 50 container carriers’ websites in 2014 and found:

- 37 of 50 appear completely open to simple attacks towards back-end systems
- six allow harvesting of usernames
- eight carriers, controlling 38 percent of global trade, allow “password” as a password to access sensitive eCommerce applications
- two carriers allow “x” as password

When chartering vessels, the operating company is often seen not to have specific cyber security requirements, says CEO Lars Jensen. A vessel and its equipment has to be considered as being just accessible as any land-based computer, he says.

The maritime industry will remain vulnerable to cyber-crime unless it develops a better awareness of ICT security and adopts security best practice, warns ESC Global Security’s head of cyber security division, Joseph Carson. “Certainly there is the possibility for AIS, GNSS, ENC and ECDIS charts to disappear from bridge screens or be modified, but the issue today is that most adversaries want to obtain data for financial gain or criminal activities.” He says that payment systems, for example, can be easily attacked using phishing scams to raise fake invoices or even to change shipping manifests in order to transport illicit goods, drugs and weapons.

Echoing comments made by World Economic Forum managing director Espen Barth Eide at Nor-Shipping last week, that “every conflict we see in the future will be a cyber-conflict,” Carson says that while the threat is indeed a real one, greater computer literacy and security awareness can reduce the risk of maritime cyber-crime by as much as 25 percent.

“The biggest risk is from human operators not understanding how to deal with or identify a possible security breach. Almost 70 percent of malware is manually shared through social media, so awareness and continuous training can have a tangible impact.”

Carson points out that the maritime industry is operating computer systems that remain unpatched for long periods, but continuous updating can prevent vulnerabilities in software from being exposed and used by adversaries.

“Approximately 99 percent of all cyber-security breaches are from known vulnerabilities with the common vulnerabilities and exposures listed in the National Vulnerability Database. About 90 percent of these breaches, however, have patches [software updates] available containing the required security fixes,” he says.


**Cyber Attacks on ECDIS, AIS**

According to Tor Svensen, maritime CEO at DNV GL, the industry has already seen its first cyber events including the manipulation of AIS, ECDIS and GPS data. Just last year, more than 50 cyber security incidents were detected in the Norwegian energy and oil and gas sector, he says.

“Ships and offshore structures are becoming more and more interconnected,” says Svensen. “In theory, all programmable components may be exposed to cyber threats, be it machinery, navigation or communication systems.”

A report last year by Marsh and McLennan notes that because it doesn’t have an inbuilt mechanism to encrypt or authenticate signals, AIS is considered to be a soft target for cyber-attack, which was demonstrated in 2013 by cybersecurity firm, Trend Micro. The firm was able to show how AIS could be compromised by preventing a ship from providing movement information, by making phantom vessels or structures appear, by staging fake emergencies, and by making it appear to other AIS users that a ship was in a false location. The online services that monitor AIS data to track the position of vessels were also misled by the efforts of Trend Micro. If, for example, a cyber-attack disabled a vessel transiting the Panama Canal resulting in blockage of the channel, it would have significant economic impact around the globe, states the report.

Russian Maritime Register of Shipping highlights that research workers from Texas University have already demonstrated the potential for changing a ship’s direction using GPS signal jamming to give false interpretations of course parameters to its navigation systems. In Africa, an unknown hacker made an intrusion into the positioning system of a floating production platform which brought about an impermissible heel and interrupted work. In another instance, unknown hackers made an intrusion into the computer network of a port to find containers to target for theft.

Last year, a research team from software security consultants NCC Group discovered several weaknesses within an ECDIS demo product, which enabled them to access and modify ECDIS files and insert malicious content. If exploited in a real scenario, these vulnerabilities could cause serious environmental and financial damage.

Yevgen Dyryavyy, security consultant at NCC Group, said that access to ECDIS on vessels is somewhat restricted, but this should not be used as a sole defence mechanism. “An ECDIS could still be accessed through a USB stick or an online chart update or even sensor compromise or other systems that's connected to the vessel’s local area network.”

Cyber security was discussed at IMO’s MSC meeting last November with some calling for the development of cyber security guidelines.
Modern ships contain highly sophisticated communications and navigation systems. Seen here is a VisionMaster FT Integrated Bridge System by Sperry Marine. Fierce storms and lashing seas are no longer the greatest threats to maritime commerce. Today’s biggest threats are stealthy, invisible and almost impossible to detect. They are called “cyber-attacks,” and they can be carried out with growing ease by astute terrorists and other adversaries who have the technical know-how to take remote control of—or interfere with the operations of—large ships, ports and oil rigs.

“Maritime cyber-attacks are no longer the stuff of science fiction. They are happening now, and the threats are growing,” says Professor Fred Roberts, director of CCICADA, a homeland security research group that is helping to lead a national effort to find solutions to this problem. “CCICADA is making this threat one of its top research priorities.”

CCICADA, a US Department of Homeland Security (DHS) University Center of Excellence, is currently working with maritime cyber-security experts around the world to research, analyze and find ways to thwart the growing threat of cyber-attacks on North American military and industrial targets.

This is an urgent task, particularly in the area of education and training, as many shippers, port operators and sea-based oil drillers have little knowledge of these threats or how to deal with them. The US Government Accountability Office underscored the seriousness of the threat in a report on Maritime Critical Infrastructure Protection, urging the DHS to take actions to better protect American sea ports from cyber-attacks.

Storms like this one in the Irish Sea are no longer the greatest threat to maritime Commerce.

In what is believed to the first event of its kind, CCICADA and the American Military University joined forces March 2-3, 2015, to host the Maritime Cyber-security Learning Seminar and Symposium at Rutgers University. Among the speakers was Captain David B. Moskoff, a US Merchant Marine Academy professor who is a national expert on the subject. He is deeply concerned about the lack of awareness of this threat, particularly in the world of maritime commerce. The upcoming learning seminar and symposium is designed to start closing that awareness gap.

Moskoff notes that modern vessels—from supersize tankers and container ships to luxury cruise liners—are heavily dependent on complex computer systems and radio-based cyber communications. This makes them exceedingly vulnerable to such attacks.

“Our increasing reliance on these systems and equipment makes us more vulnerable should they be lost or compromised,” Moskoff said in a recent article on maritime cyber-security. “Being ahead of vulnerabilities affecting navigation, machine and engine control, cargo operations and
communications is a challenge. Striving to protect all exposures to any type of event which might negatively impact such operations is paramount.”

At a July 2014 CCICADA seminar, Moskoff discussed in detail one particular threat—the denial-of-service attack—which uses jamming technology to interrupt Global Positioning Satellite (GPS) communications and capabilities. GPS technology is widely used in the maritime industry for commercial ship navigation, port operations and related activities. It is also used by the US Coast Guard to support its protection of the nation’s maritime borders. Capt. Moskoff says GPS jamming could close a major port for days, resulting in a billion dollars or more in economic losses.

In an August 2014 CCICADA teleconference and seminar, Canadian Naval Captain Peter Crain said the threat of cyber-attacks in the maritime industry is not only real, but could also have a severe impact on commerce and the economy. More than 90 percent of the world’s trade in goods is transported by ship, and in the US, shipping ports handle more than $1.3 trillion in cargo annually.

Real or potential maritime cyber-attacks have been well documented. Here are a few examples:

- In a “zombie attack,” a Chinese manufacturer stands accused of implanting malware in inventory scanners to steal supply chain intelligence.
- Hackers recently shut down a floating oil rig by tilting it.
- University of Texas researchers used a custom-made device to spoof the GPS of an $80 million yacht, throwing it off course.
- Low-cost GPS jammers available on the Internet can wreak havoc with ship navigation systems and shut down ports.
- Hackers are targeting ERP software platforms that are at the heart of most shipping companies’ critical data and processes.
- Somali pirates now view navigational data online to help select their targets, prompting ships to turn off their navigational devices.
- Criminals hacked into the cargo handling system in the Port of Antwerp, located specific containers, made off with smuggled items, and deleted evidence of the container’s presence.

For modern ships there has been a developing dependence on the proliferation of sophisticated technology that is subject to cyber-attack through radio frequency (RF) interference whether intentional, unintentional or by natural causes. These technologies include:

- ECDIS (Electronic Chart Display and Information System)
- AIS (Automatic Identification System)
- Radar/ARPA (Radio Direction and Ranging) (Automatic Radar Plotting Aid)
- Compass (Gyro, Fluxgate, GPS and others)
- Steering (Computerized Automatic Steering System)
- VDR (Voyage Data Recorder –”Black Box”)
- GMDSS (Global Maritime Distress and Safety System)
The dramatic dependence on these computer-run systems increases the vulnerability of today’s massive ships. For instance, the Triple E Maersk, soon to be launched, will be the world’s largest container ship. It will be 400 meters long and have capacity to carry 18,000 containers. Yet, it is designed to run with a crew of 13 people.

“Without question, maritime cyber-security is one of the greatest ‘unknown’ challenges currently faced by the homeland security community,” says CCICADA Director Roberts. “We need to address this issue now to protect our ports, ships and maritime transportation system.”


Front-page headlines revealing devastating cyber-attacks on government agencies and the world's largest companies have become a regular occurrence. Recent cyber-attacks reported by the mainstream media include the cyber-attack against SONY, Anthem Health Insurance, the White House, the Office of Personnel Management ("OPM"), Ashley Madison, and even the Houston Astros. As the list of companies and agencies that suffer cyber-attacks grows longer, it is clear and undeniable that no industry is safe, and any company that relies on information and communication technology ("ICT"), must take the appropriate steps to protect itself against cyber threats. Although the maritime community has not yet garnered front-page attention as a victim of a recent cyber-attack, make no mistake, the maritime industry is one of the most heavily targeted industries in the world and also suffers cyber-attacks regularly.

Targeting the Maritime Community

Like many government agencies, as well as the aerospace and defense industry, banking and health insurance industries, and even the entertainment industry, the maritime industry is a prime target of cyber-attacks and has suffered, and continues to suffer, many significant cyber-attacks. The maritime community has been able to avoid disastrous media coverage regarding cyber-attacks not because it is immune from cyber threats, lack of opportunity, or that the industry employs cutting edge cybersecurity programs and effective protocols to protect itself from cyber-attacks, but mostly because of luck, timing, and our tight-lipped community.

For example, the BP oil spill was not caused by hackers or cyber criminals, but it could have been, and such an event is likely to occur in the future. Yes, oil rigs are hackable. There have been multiple reports of oil rigs having been hacked, including at least one case where hackers were able to tilt the rig. Although no oil spill resulted, this should serve as a warning to the maritime community.

Likewise, the grounding and partial-sinking of the Costa Concordia appears to be the fault of human error, not because hackers manipulated the GPS, ECDIS, or AIS. But all vessels that rely on e-navigation and GPS, ECDIS, and AIS are susceptible to cyber-attacks, and all such systems can be manipulated by hackers and cyber criminals. There have been recent accounts outlining how both airplanes and cars can be manipulated and controlled remotely by cyber hackers, due to reliance on ICT. Vessels are no exception. It is only a matter of time before the next headline of
Cyber threats are very real and the consequences of a hugely successful cyber-attack in the maritime industry would be disastrous. However, cyber-attacks have been happening in the maritime community for years, resulting in mostly financial losses, as opposed to loss of human life or severe damage to the environment, which is of particular concern to the maritime community. In addition to recent reports regarding the hacking of oil rigs and the manipulation of GPS, ECDIS, and AIS, the bunkering community and many shipping companies continue to suffer tremendous losses due to cyber-attacks. For example, in December 2014, a major maritime company engaged in a deal to order a sea floor mining vessel in China on the back of a long-term charter. The maritime company reportedly pre-paid $10 million of the $18 million charterer's guarantee. Unfortunately, the company was a victim of a cyber-attack as it unknowingly paid the deposit into a bank account that belonged to a cyber-criminal. The matter was promptly referred to police authorities, who pursued an investigation. In an effort to better protect itself from future cyber-attacks, the maritime company also engaged a cybersecurity firm to ensure the ongoing security of its networks and to investigate the source of the cyber-attack. Similarly, as recently as this past August, hackers stole about $644,000 from a shipping company registered in Cyprus. The Limassol based shipping company received an e-mail purportedly coming from their fuel supplier in Africa requesting that money owed be paid to a different bank account than usual. The shipping company complied, only to find out that they had been defrauded when they later received an e-mail from the fuel company asking for payment.

**Cyber Regulations on the Horizon**

Since the U.S. Government Accountability Office ("GAO") issued its 2014 report on maritime security outlining the maritime community's vulnerability to cyber-attacks, the maritime community has slowly begun to recognize, acknowledge, and address the need for greater information sharing and the need to develop maritime cybersecurity regulations and guidelines. While the maritime industry does not currently have any cybersecurity regulations, change is on the horizon.

In 2015, the U.S. Coast Guard launched a year-long initiative to fully understand the cyber threats facing the industry, with the ultimate goal of developing cybersecurity guidelines. Midway through their initiative this past June, the Coast Guard issued a "Cyber Strategy," summarizing its vision for operating in the cyber domain. The Cyber Strategy discusses the Coast Guard's approach to defending cyberspace, including risk assessment and risk management and the strategic priority of protecting Maritime Critical Infrastructure, which includes ports, facilities, vessels, and related systems that facilitate trade within the United States. The Cyber Strategy offers a framework for the Coast Guard's plan to operate effectively and efficiently within the cyber domain.

In addition to the U.S. Coast Guard, the Round Table ("RT") group, comprising of BIMCO, ICS, Intercargo, and Intertanko, is also developing standards and guidelines to address cybersecurity issues in the industry. Acknowledging that all major systems onboard modern ships (main engine, steering, navigation systems, ballast water, and cargo handling equipment), are
controlled and monitored by software and reliant on ICT, the RT group has committed to developing guidelines to assist the maritime industry to better protect itself from cyber-attacks. It is reported that the RT group is in the final phase of developing a pattern for the maintenance and updating of electronic systems. Mr. Angus Frew, Secretary General of BIMCO, is noted as saying, "The standards under development are intended to enable equipment manufacturers, service personnel, yards, owners and operators, as well as crew, to ensure their shipboard computer-based systems are managed securely—and kept up-to date to protect against the ever-growing threat from exploitation by criminals."

Likewise, the IMO also has turned its attention to the very real threat of cyber-attacks and the need for cybersecurity guidance and regulations. At the 95th session of the IMO Maritime Safety Committee ("MSC"), held this past June at the IMO headquarters in London, the MSC addressed the issue of cybersecurity extensively and agreed to work on guidelines on managing cyber-related risks onboard ships and in port facilities at MSC 96. Proposed amendments to the ISPS Code were discussed, but ultimately it was decided that more time would be needed to develop the appropriate guidelines—given the current ongoing work of the industry on cybersecurity—with the ultimate goal of submitting a draft proposal or set of guidelines to present and discuss at MSC 96.

Accepting the Reality of Cyber Crime

The maritime industry faces very real cyber threats and potentially devastating fall out from its failure to address and employ proper cybersecurity measures. While the industry has been somewhat hesitant to discuss these cyber threats, cyber-attacks, and its subsequent losses, the reality of cyber-attacks in the maritime industry can no longer be ignored or denied. Accordingly, the maritime industry is on the verge of great change.

The leaders of the maritime community around the world have acknowledged the threat of cyber-attacks and have begun to develop cybersecurity guidelines and regulations. In the interim, cyber-attacks will continue to inundate the maritime community. To avoid catastrophic losses and to avoid becoming another victim of cyber-crime reported on the front page of The New York Times, it behooves all companies in the maritime industry to ensure they have the best cybersecurity protections available, and remain diligent in the fight against cyber-crime. Cyber-attacks are very real, and while regulations are on the horizon, cybersecurity protections are available to help guide us today.

*The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.*


*Compromising the cyber integrity of the network threatens every user and every system on your ship or in your building. Violating security best practices, circumventing security policies, carelessness and falling victim to social networking exploits opens the door to cyber adversaries who can exploit vulnerabilities which may directly impact our Navy's warfighting*
Cyber foes are no longer just recreational hackers in pursuit of bragging rights. They are cyber-criminals, cyber-terrorists and nation-states who are in constant pursuit of access to our systems. They can corrupt our Navy's data, shut down our networks and business systems, steal our science or technology and compromise the systems that run our ships, aircraft and weapons—at keystroke speeds.

Each of us stands guard on our Navy's Digital Quarterdeck. To improve our Navy's cybersecurity and successfully detect, prevent and resolve cyber persistent threats, you need to understand important stages of how adversaries can compromise our defenses.

**Stage 1 Recon**

During cyber adversary work-up periods, adversaries learn about the vulnerabilities of their target. Prior to an incident, they will gather information about the targeted networks, their systems, personnel, logistics and warfighting capabilities. They will employ many techniques, but interacting with their targets online is often the easiest method due to the volume of freely accessible information posted to popular social networking, media and web sites. Well-known, highly successful techniques to gain initial network access include:

* **Social Engineering and Complacency** - Adversaries rely on human interaction and are often successful due to their victims violating established security policies and procedures. Their goal is to get you to relax your vigilance to the point where you feel comfortable or compelled into surrendering personal or confidential information. This information could enable them to access sensitive data without your knowledge. Cyber criminals might trick you into visiting a webpage or plugging an unauthorized device (USB memory stick, CD/DVD, hard disk drive, cell phone charger, gaming console) containing malicious code into a computer on the network. By successfully piggy-backing through personnel checkpoints, thereby obtaining physical/close access to our networks, bad actors can also connect these devices to our workstations themselves.

* **Phishing ("fishing") Email** - Although known by many names depending on the targets and medium used, adversaries will send what appears to be a legitimate business or trustworthy e-mail from someone you know. It will contain a sense of urgency and a web site link in the body or in an attachment. By clicking on the link, opening the attachment, or visiting a referenced web site, you might be directed to a realistic but fraudulent website that may prompt you to provide credentials, financial information or Personally Identifiable Information (PII). Alternately, you might be directed to another web site where additional bad software (malware) will be deployed onto your now compromised computer. Once the adversary owns your computer, you may be actually forwarded to the real site and you will never suspect a problem.

* **Watering Hole** - Adversaries will target specific interest groups or organizations. They profile victims and observe the kind of websites they visit or the social media circles they frequent. Then, identify a vulnerability on one of those websites, compromises the legitimate site and wait silently for victims. Users who visit a watering hole site are stealthily redirected to another site and exploited by the adversary through the implanted malware. The computer is now compromised and often the victim will never see the incident.
Stage 2 Intrusion and Enumeration
As a result of falling victim to social engineering tactics, complacency, poor judgment, disregard for mandatory policy or unauthorized computer use, the network is now compromised - Set Cyber General Quarters! On your watch, the adversary has gotten past your digital quarterdeck. Once inside the network, a stealthy intruder will blend in with normal traffic, making detection very difficult.

Similar to the recon of the network's perimeter for access points, the adversary now begins identifying existing security flaws within the network's lifelines. Intruders will covertly deploy their cyber tools. Software will be used to probe computers, identify vulnerabilities and scan the environment to put together a cyber map for better understanding your network terrain. If it has power and it communicates, it is probably accessible.

Stage 3 Malware Insertion and Lateral Movement
Adversaries will establish persistence by creating additional points of presence throughout your network by using software such as remote access Trojans (RAT), which are more commonly known as backdoors. They will attempt to move laterally, spreading across the network and hiding in the deepest areas in the network while lying dormant. Other adversaries will implant software that captures key strokes and grabs passwords, which helps them crack accounts that give them more privileges on your network and get the keys that will give them access to mission critical information, sensitive data, valuable intellectual property or warfighting/platform control systems.

Once the intruder has persistent presence, they can degrade or disrupt network activity at whim. Determining the full scope of an intrusion can take months to years, and we can never fully guarantee that all backdoors and other software have been completely removed.

Stage 4 Data Exfiltration
The hull has been breached. The digital integrity of the network has been fully compromised. Once an adversary determines that they have established reliable network access, they can move sensitive information to an outside location. Even though files and passwords are often encrypted, encryption can be cracked outside of the compromised environment. When that happens, intruders can then identify alternate targets and re-engage, or use the information obtained to go after another victim.

Stage 5 Clean Up
The final step of a cyber incident is for the intruder to clean up. Some merely disconnect, unconcerned that the victim may eventually find out what happened. Other more sophisticated actors will attempt to rid all systems in the network of any forensic evidence or trail of compromise. The intruder will delete data, over-write data, remove implanted files, clean up event logs, deactivate alarms, roll back software updates, delete backups or erase hard drives. Their goal throughout the entire incident is to erase any trace that the incident ever happened or make it look like a computer glitch while maintaining backdoors they can revisit at any time to exploit our systems further.
Each of us is on the front line of the cyber warfighting domain. We are all sentries guarding a potential entry point on the perimeter of the Navy's network and are charged with the defense of our information systems' warfighting capability. Each of us has a finger on the keyboard and mouse and it only takes one lapse of judgment, mistake or a one click misfire to give it all away. You are our greatest asset, and our greatest vulnerability.

No matter what the intent, whether financial, to steal intellectual or state secrets, or install malicious software that will be activated during the next conflict, our cyber adversaries are determined, intelligent and have little chance of being identified and little concern about reprisal.

Cyber threats are real. Traditional cybersecurity measures, such as defense-in-depth, firewalls and antivirus, cannot protect against the human element of advanced persistent threats. However, you can. Do not engage in practices dangerous to our Navy's cybersecurity. The CNO has made it clear that "cybersecurity is a commander's business" and requires all hands to keep the Navy and our nation safe. It's important that each of us treat our network as the weapon system.

The mission of Navy Cyber Defense Operations Command is to coordinate, monitor and oversee the defense of Navy computer networks and systems and to be responsible for accomplishing Computer Network Defense (CND) missions as assigned by Commander, U.S. 10th Fleet and Commander, U.S. Cyber Command.

Along with all the hype and talk about autonomous ships and big data has inevitably come a debate highlighting cyber-security and the risk of ships being deliberately steered off course. Experts will tell you, and can demonstrate, how easy it is to take control of something that is remotely operated if the security is inadequate. They can also show you how easy it is to gain access to data in order to change crew and cargo manifests.

Today’s very real risks to shipping mirror those of many other businesses, and yet the industry is barely taking note. Risks involving data theft and deception were highlighted recently by the loss of millions of dollars by one of the industry’s suppliers, Konecranes.

In August this year, Konecranes, a Helsinki-listed heavy lift and crane specialist with equipment for container ports and shipyards, admitted it was the victim of fraud — a case in which it lost about $19m. Criminals stole digital identities to con a subsidiary of the company, which subsequently made unwarranted payments.

A little education can go a long way in creating awareness of the risks, says BIMCO security officer Phil Tinsley, and helping to avoid becoming a victim of similar crimes. This has also been echoed by Joseph Carson at Estonian security firm ESG ESC Global Security. He is a cyber-security expert who has worked with leading IT security outfits, including Symantec, and joined the private security firm when it expanded its focus into cybercrime. Shipping faces the same challenges as other industries, but the scale is different, Mr. Carson says.

More worrying, however, is how far behind shipping is in awareness of the basic risks compared with other industries, he adds. This may be because ship owners have traditionally remained
quiet and are generally not in favor of open dialogue due to reputational risk. It may also be because until the past decade, they had limited cyber-exposure, but with satellite bandwidth now cheaper and a lot more accessible, vessels — particularly complex ones — have become extended offices, and are therefore exposed to the same risks.

Risk awareness does not only include recognizing one’s own exposure, but that of partners, customers and suppliers due to increasing digital connections. It is, says Mr. Carson, relatively easy for criminals to gain this kind of sideways access. In Europe, there is the new General Data Protection Regulation, established as the region strengthens existing directives that have previously been used as guidance. While the regulation has a strong consumer or personal protection element, it does create, through a mandatory breach notification, the requirement for any company that experiences data theft, or any other infringement, to disclose it or risk a potentially large fine. The law is aimed at companies involved in critical infrastructure — and in Europe, maritime is seen as a critical infrastructure — but it will also impact supplier companies, particularly those working with ship owner data.

(FBI 2015) DHL Customers Being Targeted in New Phishing Email Scam (16NOV2015) By Comodo editor

With the holiday season fast approaching, the shipping of packages and gifts will reach a fever pitch over the next two months. This is the time when cyber criminals are looking to strike, not only stealing critical financial information, but looking for ways to steal personal information.

The Comodo Antispam Labs (CASL) team has identified a new global phishing threat, targeted specifically at the 2.5* million global businesses and consumers who use DHL shipping. The fake DHL phishing emails are sent from ‘DHL Worldwide’ containing the subject line “DHL Shipping Delivery Tracking Number.’ Trying to represent colors and logos of DHL, the “fake DHL” phishing email is designed to capture logins and passwords to DHL accounts and package tracking information. The phishing email asks recipients to verify the tracking process for their impending packages, deliveries and shipments.

The Comodo Antispam Labs team identified the DHL phishing email through IP, domain, URL analysis, and image analysis. “Through specific IP and URL analysis – as well as the Comodo Antispam Labs’ continuous monitoring and scanning of data from the users of Comodo’s Internet security systems, our team was able to identify this specific phishing email scam and alert the public to it,” said Fatih Orhan, Director of Technology for Comodo and the Comodo Antispam Labs. “As a company, we work diligently in creating innovative technology solutions that stay a step ahead of the cyber criminals, and keep enterprises and IT environments safe.”

Image screen shots and more information on the DHL phishing scam can be found below. The Comodo Antispam Labs team is made up of more than 35 IT security professionals, ethical hackers, computer scientists and engineers, all full time Comodo employees, analyzing and filtering spam, phishing and malware from across the globe. With offices in the US, Turkey, Ukraine, the Philippines and India, the CASL team analyzes more than 1,000,000 potential pieces of phishing, spam or other malicious/unwanted emails per day, using the insights and
findings to secure and protect its current customer base and the at-large public, enterprise and Internet community.

If you feel your company’s IT environment is under attack from phishing, malware, spyware or cyberattacks, contact the security consultants at the Comodo Antispam Labs: https://enterprise.comodo.com/contact-us.php. Although the email appears to be from “DHL Worldwide,” the recipient needs to be aware that the actual email address itself is not a DHL email.

When the potential phishing victim clicks on the DHL.com/tracking link in the email (above), it takes the user to a new landing page – also trying to represent DHL (below). In just one click, the cyber thieves are now trying to steal password and log in information. After the phishing victim simply verifies their email address and enters the password, a page opens with the text appearing “Your email has been updated” – making the victim feel as if all was an authentic transaction. In actuality, the log in and password have now been sent to the cyber criminals and they can immediately begin using that to access account and data information, or selling that information on the black market.

**NOTE** from COMODO ANTISPAM Labs: because this was an actual intercepted email, the actual email address it was sent to has been removed to protect the original recipient and has been replaced in this screen shot to “thisis@fakeemail.com”. For the System IT Administrators who think their IT may be susceptible to the fake DHL phishing email, the address, malicious URL, domain and IP address to be aware of is below:

- The domain that the phishing site is hosted on is conceptsolutionind.com
- The IP address is 192.185.56.51 which resides in United States, in Texas
- Registrant Country: India
- The From domain is werrtonholdings.com.au
- The mail is sent from IP: 216.151.170.2 and it belongs to:
  - Shared-hosting.webminders.com which is a hosting site and not a private IP

*(FBI 2015) Adware Program Vonteera Blocks Security Products with Simple Windows UAC Trick (23 NOV 2015) By Lucian Constantin*

A well-known adware program is preventing users from installing antivirus products by leveraging a Windows feature that was designed for security. The program, known as Vonteera, abuses the digital signature check performed by the Windows User Access Control (UAC) for executable files.

UAC prompts users for confirmation whenever a program wants to make a system change that requires administrator-level privileges. It therefore prevents malware from silently gaining full system access if executed from a limited user account.

Depending on whether an executed file is digitally signed by a trusted publisher, the UAC displays confirmation prompts indicating different levels of risk. For example, if the file is
unsigned, or is signed with a self-generated certificate that Windows can't link back to a trusted certificate authority, the UAC prompt will have a yellow exclamation mark.

However, if the file is signed with a certificate that was blacklisted, UAC will simply block the file from running and a red warning will be displayed. It seems that the creators of Vonteera, whose purpose is to hijack browsers and display ads, have figured out that they can abuse this UAC behavior to prevent users from installing security products.

The program copies 13 digital certificates that were used to sign antivirus programs and security tools to the "Untrusted Certificates" store in Windows, researchers from security firm Malwarebytes said in a blog post. The blacklisted certificates are from Avast Software, AVG Technologies, Avira, Baidu, Bitdefender, ESET, ESS Distribution, Lavasoft, Malwarebytes, McAfee, Panda Security, Trend Micro and ThreatTrack Security.

Vonteera creates a service that periodically checks if these certificates are present in the "Untrusted Certificates" store and adds them back if they're not. Fortunately, this blacklisting of vendor certificates is only partially effective, said Bogdan Botezatu, a senior e-threat analyst at antivirus vendor Bitdefender. The technique only prevents new product installations or the execution of stand-alone removal tools that need administrator privileges. System drivers and services created by antivirus products that are already running would not be affected, he said.

However, if the user already has an antivirus running and Vonteera has managed to make these changes, it means that the product already failed to detect it and the user would need to install another tool to remove it -- one that might now be blocked.

Vonteera is quite persistent and intrusive, so users would have a hard time getting rid of it manually. The program creates multiple scheduled tasks to ensure its execution and to display advertisements on a regular basis. It also registers a system service, installs rogue extensions in Internet Explorer and Google Chrome and alters the browsers' shortcuts to automatically open a URL when clicked.

Affected users have several options to bypass Vonteera's changes to the Windows certificate blacklist so they can install an antivirus product. They could disable UAC entirely, but this is not recommended because it reduces the system's security.

They could also manually remove the certificates from the "Untrusted Certificates" store by using the Windows Certificate Manager tool, but then they have to act fast before Vonteera puts them back. This can be done by hitting the windows key + r to open a Run prompt then typing certmgr.msc. In the left panel they can browse to Untrusted certificates > Certificates and remove certificates that have an antivirus vendor's name.

Finally, they could use a trick that uses scheduled tasks to bypass UAC prompts in order to install their desired antivirus tool, use it to remove Vonteera, then manually remove the blacklisted certificates, the Malwarebytes researchers said.
Because of this intrusive behavior, Malwarebytes has changed Vonteera's classification from a potentially unwanted application to a clearly malicious application, detecting it as a Trojan. Other antivirus products including Bitdefender and ESET also have detection routines for it.

(FBI 2015) Crafty Spear-Phishing Campaign Uses Terror Attack to Increase Proficiency (23 Nov 2015) By Doug Olenick

Cyber-criminals are using the fear generated from the recent wave of terror attacks to target corporate offices in the Middle East and Canada with spear-phishing attacks.

One of the more sinister aspects of this campaign is the amount of obfuscation being used by the attackers, to include the names of real security officials and even some legitimate attachments.

Symantec's Lionel Payet said in a blog post that the company had noted malicious emails falsely using the address of the Dubai Police Force in the United Arab Emirates to convince the recipient that the email contained official correspondence on how to avoid terror attacks. To increase the email's validity the crooks used the name of the lieutenant general who heads the Dubai police and is head of security for the country.

The spear-phishers then double down on their duplicity by including one legitimate attachment.

“The emails come with two attachments, one of which is a PDF file that is not actually malicious but acts as a decoy file. The malware resides in the other attachment, an archive, as a .jar file,” Payet wrote.

The phishers are using a multiplatform remote access Trojan called Jsocket, which is a new tool from the same group that created AlienSpy RAT.

“While the group behind this campaign mainly targeted UAE-based companies and employees, we have also seen similar spear-phishing runs targeting three other countries: Bahrain, Turkey and, more recently, Canada,” the blog post said, adding that Symantec believes the group is expanding its efforts further and it expects to see new countries targeted.
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)
- 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:


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.