**March 9, 2017**

**Maritime Cyber Security**

[**http://www.mtinetwork.com/taking-maritime-cyber-security-seriously/**](http://www.mtinetwork.com/taking-maritime-cyber-security-seriously/)

* **Port of Antwerp**
  + **Hackers working with drug smuggling gangs**
    - **Breached digital tracking**
    - **Located containers filled with drugs**
    - **Drivers picked up containers ahead of time**
  + **Port discovered truck which was broken down**
  + **Two years of operation**
    - **No major repercussions to Port of Antwerp or companies**
* **Potential hazards**
  + **Accessing vessels AIS**
    - **Prevent vessels from providing movement details to shore**
    - **Cause navigation operators to see “phantom” targets potential collision**
  + **Drilling Rigs**
    - **Forced to suspend drilling operations**
    - **Risk of driving off location via DP or VMS/PMS**
    - **Risk of equipment failure or under/over performance**
  + **Cargo/Container Ships**
    - **Container lines entire cargo database wipe out or manipulated**
      * **Container number**
      * **Location**
      * **Place of origin**
  + **Companies not reporting cyber-attacks**
    - **Losing contracts**
    - **Fear of notifying client confidential information compromised**
    - **Not sure a cyber-attack even happened**
* **Ways to prevent cyber-attack**
  + **Top-down effort thru policy**
    - **Set strong user access controls**
    - **Set strong network access controls**
    - **Perform regular backups**
    - **Keep software up-to-date**
  + **Train employees on how to recognize cyber-attacks**
    - **Online courses**
  + **Policies on USB memory stick usage**
    - **Lock out USB drives with key access to designated person**
    - **Fill out permit to work with risk assessments in place**
    - **Scan memory sticks including third party groups**

[**http://researchcenter.paloaltonetworks.com/2017/03/gov-cdans-2017-keeping-cybersecurity-skills-sharp-cyber-range/**](http://researchcenter.paloaltonetworks.com/2017/03/gov-cdans-2017-keeping-cybersecurity-skills-sharp-cyber-range/)

* **Cyber Defense and Networks Security**
  + **Cyber Test Systems**
  + **Cyber Range** 
    - Used by technologists – network engineers, cyber operations professionals, and others charged with some level of responsibility for their enterprise’s security
    - Customize sophisticated testing protocols in hours
    - Expose systems and networks to realistic nation-state threats
    - Conduct force-on-force exercises
    - Evaluate the latest techniques in cyber protection
  + **Protection from**
    - Recent ransomware such as: Petya Goldeneye, Merry Christmas, Cerber, Sopra, CryptoMix, Osiris variant of Locky
    - Recent web exploit kits, such as Magnitude, KaiXin, Rig-E, Rig-V, Sundown
    - Phishing attacks
    - Malicious domains and websites
    - Exploits of vulnerable clients and servers
    - DDoS attacks including DDoS, RDoS, and DRDoS attacks – just like the Mirai botnet DRDoS attack
    - Recent botnets’ command and control, such as Kelihos botnet and Mirai botnet
* **Palo Alto Networks**
  + Palo Alto Networks is a regular contributor to vulnerability research
    - Microsoft, Adobe, Apple, Google Android and other ecosystems.
    - Identifying these vulnerabilities, developing protections for customers, and sharing the information with the security community
    - Removing weapons used by attackers to threaten users, and compromise enterprise, government, and service provider networks.
* **Ignite 2017**
  + - Hands on workshops
    - Ultimate test drives
    - Breakout Sessions
    - June 12th- June 15th

[**http://researchcenter.paloaltonetworks.com/2017/01/unit42-farming-malicious-documents-unravel-ransomware/**](http://researchcenter.paloaltonetworks.com/2017/01/unit42-farming-malicious-documents-unravel-ransomware/)

[**http://researchcenter.paloaltonetworks.com/2017/03/unit42-blank-slate-campaign-takes-advantage-hosting-providers-spread-**](http://researchcenter.paloaltonetworks.com/2017/03/unit42-blank-slate-campaign-takes-advantage-hosting-providers-spread-)

* **Malicious Spam(Mal-spam) “Blank Slate” Campaign**
  + - Attacker’s botnet sends malspam to the intended recipient.
    - User ignores security warnings and opens the zip archive included in the malspam.
    - User ignores security warnings and manually extracts either a Microsoft Word document or a JavaScript (.js) file.
    - User ignores warnings and manually enables macros for the Word document or user double-clicks the .js file.
    - Word macro or .js file retrieves a ransomware executable from a web server.
    - Word macro or .js file executes the ransomware on the user’s computer in the user’s security context.
  + Campaign using emails with no message content and a zip archive to spread ransomware
  + Farming Microsoft Word documents in AutoFocus
    - 500 domains were used
    - Used ransomware variant “Sage 2.0” spin-off of CryLocker
    - Launch a PowerShell process to download the actual ransomware using an evasion technique
    - ‘The idea behind the evasion technique is to bypass pattern or string matches that prevent process launching by using the Windows command-line escape caret character injected between your regular characters to break up commands such as “powershell” and “executionpolicy”’
  + Example: ‘You tried to block “powershell”, it would fail because the carets have broken up the word, but it will have no impact on Microsoft Window’s actual processing of it. The Microsoft Word document contains an obfuscated macro that puts together this command and executes it, which subsequently downloads the ransomware file and runs it. ‘
  + **Macro malware** usually hides in Microsoft Word or Microsoft Excel documents. These malicious documents are sent as spam email attachments, or inside ZIP files attached to spam emails. They use files names designed to entice you into opening them.
  + read.php?f=0.dat
    - Malware-Traffic-Analysis
    - For each “person” there were multiple domains that are tied to that identity
  + **PowerShell** (including Windows **PowerShell** and **PowerShell**Core) is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language built on the .NET Framework.
  + “Blank Slate” keeps getting away with creating new domains
    - Email
      * Free email services
    - Phone number
      * Burner phones
    - Credit Card
      * Stolen credit card information
  + Criminal Accounts on Hosting Providers is short lived-a week at most
    - When a server is taken offline-criminals easily establish a new server link
  + Palo Alto Networks uses *Wildfire* to identify Macro Malware

**Cal Maritime Academy Maritime Cyber Security Discussion**

* Women in Maritime Leadership
* Speaker: **Lee Rosenburg**
  + Consulting company
    - Homeland security emergency preparedness
    - Retired from the navy
  + CIA hacked
    - Found CIA hacks
  + NRC-IC.org
* Speaker: **Cynthia Hudson**
  + Hudson Analytix <http://www.hudsonanalytix.com/>
    - Philadelphia area
    - Costco Busan
  + Security Assessment
    - Outstanding woman in maritime port
  + Max Bobbies
    - Wrote presentation
  + Data Integrity
    - Posting, altering, modifying stored data, transmitting data, theft
  + Vulnerabilities
    - Personal, professional, systematic
  + Reasons for hacking
    - Info
    - Legacy systems
    - Money
    - Different languages/cultures/Global trasportation
  + Hackers
    - Individuals
    - Hacktivists
    - F. Intelligence
    - Criminal rings
    - Competitors
  + Trench time
    - Develop with other hackers/methodology
    - Black Hat
  + Donald-Duck
    - Any way of hacking into system/secondary victim
  + Threat convergence
    - Drug traffics
    - Hacking technique physical access
  + “The Daily Show” campaign
    - In Nigeria
    - Supply chain targeting
  + IRISL Hack (2011)
    - Servers compromised
  + Practical recommendations
    - Begins at top
    - Assess-realign-remediate-measure&report
    - Cyber maturity
    - Train and exercise
* Speaker: **Brian Rodriguez**
  + NCRIC (Northern California Regional Intelligence Center) <https://ncric.org/>
  + Cyber intelligence teams
  + Unified Dataset
* Speaker: **Maureen Johnson**
  + US Coast Guard
    - Vessel inspections USCG
    - Marine Safety
    - Compliance inspections
    - First responder
    - Cyber risk management
  + Concerned with loss of life
  + Damage to equipment
  + Catastrophic disruptions to MTS
  + Major vulnerabilities 20% of identified control system networks
  + GPS Spoofing
    - Feed faulty timing to vessel
    - Cause vessel to change course
    - Gain control of nav system
    - Low cost equipment
  + ECDIS vulnerabilities
    - Connected with shipboard systems and sensors
    - Chart updates loaded via internet/CD/USB
  + Ransomware
    - Industrial control systems-water treatment plant
  + Cyber Risk
    - Vulnerability increases with every new device
    - Threat is unlimited
    - Likelihood high
  + Cyber hygiene
  + Counter-measures
    - Update anti-virus
    - Software patches
    - Change password
    - Educate and train workforce
    - Eliminate unnecessary data
    - Study threat landscape
  + What kinds of systems within the MTS are at risk
    - Engine rooms
    - Bridge control console
    - Badge readers
    - Vital cargo machinery
    - Passenger screening equipment
  + DHS
    - NCCIC-Cyber communications integrations center
    - ICS-CERT-Cyber emergency response team
  + ***CSET-Cyber security evaluation tool***
* Enrique Alvarez
  + FBI
    - Counter-Intelligence
    - Cyber Security Intrusion Squad
    - Intelligence Officer

**Case Studies**

* Business Email Compromise(BEC)
  + Ask questions
  + Sometimes not sophisticated email attacks
    - Wrong emails
  + 20-60k loss
  + Insider threats
    - Sociological company behaviors
      * Disgruntled employees
    - Inadvertent threat
* Redundancy
  + In case equipment is compromised
* International hack like a pirate day
  + Pirates raid ships they have a good idea what they are after
    - Hackers break in online, steal ships manifests and sell on dark web
      * Area of the internet accessible through TOR
      * Created by USG
      * Masked IP addresses
      * Criminal enterprises
      * Customer service reps, rate transactions, very legitimate
    - Dark Web has Brokers to sell information
      * Hard to disrupt
      * FBI
      * Silk Road
      * SpotNet-Delivering spam, Ransomware

Speaker: **Dr. Brad Thayer: Cybersecurity**

* Cyber warfare deterrence
  + Strengthen forensics
  + Establish norms
  + Create policies and mitigations
* Cyber is a new and major avenue of attack and espionage
* United States and Allies need to deter CAN and give empirical evidence publicly available
* Major Cyber Attacks
  + JCS and OPM
  + Solar Sunrise
  + Georgia
  + Night Dragon
  + Stuxnet
  + Shamoon
  + White House
  + Ukraine
  + APT 29 Cozy Bear
  + APT 28 Fancy Bear
* April 2007 Estonia
  + Soviet Monument-offensive to Estonian’s
    - Estonians moved it to a cemetery
    - Russian government performed cyber attacks
      * Protests from Estonians
* Deterrence Theory
  + Military Capabilities
  + Credibility
  + Political Variables
  + Will Power
* Challenges of deterring cyber warfare
  + Anonymity of cyberspace
  + Plausible deniability and “independent” actors
  + Covert development programs
  + Uncertain consequences of some attacks due to
    - Target and/or weapon unpredicatability
    - Potential for major collateral damage or unintended consequences
      * NATO’s Allied Force 1999 war with Yugoslavia
* Strengthen Forensics
  + Wide array of technologies and scientific disciplines to conduct evidence
  + Instill doubt in foe’s mind
* Cultivate beneficial norms
  + *International Strategy for Cyberspace*
    - “clearly agreed-upon norms for acceptable state behavior in cyberspace”
    - Few norms in cyber realm
    - Tallinn Manuals 1.0/2.0 Important Steps
    - Lover evidentiary standards for attributing cyber attacks could help improve ability to hold suspected cyber actors at risk
* Develop Capabilities and Declaratory Policy
  + Showing resolve: communicating a clear declaratory policy
  + Demonstrating Offensive Cyber Operations(OCOs)
    - Credible OCO options for retaliation-in-kind will enhance US deterrence of major cyber attacks
* Mitigate Harboring of Independent Cyber Attackers
  + No more HIDDEN LYNX-“Independent” Hackers in China
  + Reduce plausible deniability
    - Incorporate this in US
    - Designate “state sponsors of cyber attacks” with associated sanctions, just as state sponsors of terrorism are identified
    - Sanctioning individuals
    - Expelling diplomats, denying access, as Obama did to Russia after GIRZZLYS STEEPE
* Future of cyber warfare questions
  + What ways cyber battlespace analogous to the physical domains of land, sea, air and space
  + How widely will cyber war proliferate
  + What are lessons of Iran’s and North Korea’s Rapid Development of Cyber Capabilities
  + Will cyber be a weapon wielded by a relative few number of states
  + What lessons are there from the past for arms control in the cyber domain
* Challenges for deterrence in cyber realm
  + Improvements occurring
  + More analysis needed