Evolving Cyber Threats to the Marine Transportation System

Brett Rouzer
USCG Cyber Command
(202) 372-2871
Brett.R.Rouzer@uscg.mil
“Cybersecurity is one of the most serious economic and national security challenges we face as a nation…”

- President Obama, February 2013

“All sectors of our country are at risk...the seriousness and the diversity of the threats that this country faces in the cyber domain are increasing on a daily basis.”

- DNI Director Clapper, March 2013

“Cybersecurity is a matter of homeland security...we are all connected online and a vulnerability in one place can cause a problem in many other places...cybersecurity is one of our most important missions.”

- Secretary Johnson, April 2014

“Cyber affects the full spectrum of Coast Guard operations...it cuts across every aspect of the Coast Guard. We all have a role in cybersecurity and protection of our networks, and we must treat them like the mission-critical assets that they are.”

- Admiral Zukunft, September 2014
The Coast Guard is the Sector Specific Agency (SSA) for the Maritime component of the Transportation Sector

- 1 of the 16 Critical Sectors
- Collaboration with our partners in TSA and DOT
- Protect maritime sector from all threats (physical, personnel, and cyber)
Why Maritime Trade is Important

- 95% of all U.S. overseas trade through 360 ports
- $1.3 trillion in cargo annually
- 7,000 oceangoing vessels made 55,560 port calls annually
- Secure ports support Homeland Security and National Defense Ops
Intermodal Touch-points
Maritime Disruptions on MTS have proven costly

- These incidents reflect cost of a maritime disruptions.
- These may not have been caused by a cyber-based failure, cyber incidents can have similar or greater consequences

- 1989: Exxon Valdez, $7+ billion dollars
- 2002: West Coast port shutdown, $11 billion dollars
- 2007: I-35W bridge collapse, $300 million dollars
- 2010: Deepwater Horizon, $37+ billion dollars
- 2013: USS Guardian, $300 million dollars
Ships Then
Cargo Operations Then
Cargo Operations Now

- Cargo handling equipment at the port/railway interface
- Commercial Long-Haul Trucks
- Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)
- Container Cranes (or liquid cargo handling systems at oil, chemical and LNG terminals) at vessel/port interface
- Automated cargo handling equipment, vehicles and similar conveyances
- Automated Cargo Container Tracking Systems
- Shore-based systems that directly support safe vessel operation and navigation:
  - GPS
  - Lock operation
  - Communications
  - Maintenance and management
  - Systems aboard USCG vessels, tugs, fire boats, port police
  - Pollution response systems
- Terminal Operating Center (financial, communications, customs, security and other back office functions)
Differing Perspectives on Security

Asset Owner’s Perspective

Cyber Threat Actor’s Perspective
Types of Cyber Threats We are Facing

- Hackers/Intrusion Sets
- Phishing
- Social Engineering or Elicitation
- Malicious Code
- Watering Holes
- DDoS/SQL Injections
Threat Actors

- Nation States
- Insiders
- Hacktivists
- Criminals
- End Users
Cybercrime as a Service

How much does it cost to buy a cyber attack?

- DDOS Attack
- Scanning/Penetration Testing
- BOTNET
- Zero Day Exploit

Consulting services such as botnet setup
($50-$100)

Infection/spreading services
($1.00 per 1K installs)

Botnets & Rentals
[Direct Denial of Service (DDoS) $535 for 5 hours a day for one week], small spam
($40 / 20K emails) and Web spam ($2/30 posts)

Quality Assurance vs. Detection
(Crypters, Scanners - $10 per month)

Affiliate Programs
(55% per day is possible)

Onshore & Offshore Hosting – Virtual Private Servers
($6 per month)

Bulletproof/Past Flux hosting and
VPNs & reverse proxies
($60 per month)

Blackhat Search Engine
Optimization (SEO)
($600 for 30K spammed backlinks)

Inter-Carrier Money Exchange &
Mail services
(25% commission)

CAPTCHA Breaking
($1/1000 CAPTCHA) – Done through recruited humans

Crimeware Upgrade Modules:
Using Zero Modules as an example, range anywhere from $200 to $10
Hackers Used to Facilitate Drug Smuggling

By breaking into the offices of a harbor company, the criminals could install key-loggers to take control of computers.

Computers of container terminal were hacked so the containers that contained drugs could be monitored.

MODUS OPERANDI

1044 kilos cocaine/1099 kilos heroin

By means of false papers and a hacked pin code, the drivers were able to pick up the container at a location and time of their choosing.
Insider Threat – Malware via USB Device

What happened?

- Targeted attack against refinery
- Disgruntled employee loaded malware on company computers
- Impact to business systems
- Remediation required 3rd party assistance
Oil Rig Stability

What happened?

- Attacker managed to tilt floating oil rig off the coast of Africa
- Facility forced to shut down
- One week to identify cause and mitigate effects

Source: Reuters 23 April 2014
What happened?

- GPS disruption lasting for over 7 hours
- Disruption caused two ship to shore cranes to cease operations due to lack of position data
- Operation of two additional cranes degraded
Powerful WiFi devices detected on foreign flag ships

- Many antennas have a range of several miles
- Several antennas connected to computers running “password cracking” software
Industrial Control Systems (ICS)

**BlackEnergy**
- Sophisticated campaign
- Ongoing since at least 2011
- Highly modular
- Targets human-machine interfaces (HMI)
- Modules search out network-connected file shares and removable media for lateral movement

**Havex**
- Remote Access Trojan
- Multiple infection vectors (phishing, website redirects, watering hole attacks on ICS vendor websites)
- Targeted energy and oil sectors
- ICS/SCADA scanning
Types and Impacts of Exploiting ICS

- **Direct physical damage to affected equipment and systems...**
  - by exploiting an ICS, the controlled mechanism can fail with catastrophic results, damaging a single piece of equipment, interrupting a larger system, or disabling or destroying an entire ship.

- **Small-scale, local disruptions...**
  - which damage or interrupt individual systems or single ships within a single organization, without widespread impact beyond the affected function or service.

- **Injury or death to operators, passengers or the general public.**
  - An incident can affect a single operator or a larger number of crewmembers or bystanders. Targeted attacks on a safety-critical safety can result in a fire or explosion that injures or kills hundreds.

- **Catastrophic disruptions to the transportation system.**
  - A vessel sunk in a shipping channel, an explosion at an oil or LNG facility, sabotage to canal locks, or a series of mishaps involving cargo container cranes in critical ports can have long-term impacts to the safety, stability and reliability of elements of the transportation system.
GPS Jamming and Personal Privacy Devices

- Increased use of Personal Privacy Devices (PPDs) to mask user position from GPS-based tracking systems
  - Employee tracking (Commercial Trucking Sector)
  - Personal tracking
  - Rental cars
  - Prisoners ankle bracelet
  - Stolen Vehicles - cars/trucks
  - Cell phones / Drug dealers
- Growing market for low-cost GPS jammers
  - Many devices are battery-operated or can be plugged into a cigarette lighter
- Examples: gpsjammers.net, jammer-store.com, chinavision.com, others

Volpe, 2013
GPS Spoofing

- University of Texas at Austin “Proof of Concept”
- Attacker transmitted spoofed GPS signal
- Signal overrode civilian GPS
- Obtained control over primary/back-up GPS (no alarms on radar, gyro, or compasses)
- “Attacker” gained navigational control of ship and redirected course
Final Thought...Saudi Aramco

- National oil company of Saudi Arabia
- One of the largest producers of oil in the world
- Targeted cyber attack
- Data destroying malware
- 30,000 computers turned into paperweights

What would your organization do if all of your company’s computers stopped working?
ACT
Achieving Cybersecurity Together

“It’s our Shared Responsibility”. 