Amenazas y retos en la ciberseguridad marítima

Jose M. Fernandez, Ing., Ph.D.
Bastionnage Consulting Inc.

IALA WWA Seminario de ciberseguridad – Diciembre 2021

Esquema de la presentación

- Definiciones genéricas
  - Riesgo, riesgo cíber, ciberseguridad
  - Diferentes tecnologías cíber
- Riesgos cíber dominantes en TI/TO
- Tecnología cíber en sectores verticales marítimos
- Riesgos cíber específicos al ámbito marítimo
  - Potenciales actores de riesgo
  - Vulnerabilidades conocidas
  - Potenciales escenarios de ataque
- Retos inherentes a la ciberseguridad marítima
- Conclusiones (prioridades)

Definiciones de riesgo

- Cualitativo
  - Actor de riesgo
    - Adrede v. accidental
  - Escenario
    - Secuencia de acontecimientos
    - Con consecuencias negativas sustanciales ➔ Impacto
- Cuantitativo
  - Riesgo = probabilidad * impacto
    - Impacto = “coste” cuantificado del acontecimiento (monetario, tiempo, vida, etc.)
    - Probabilidad = capacidad * oportunidad * motivación

Ciberseguridad – Definición

- Blanco del ataque = “Bienes informáticos”
  - Sistemas: cualquier combinación de ordenadores, redes, electrónica programable, etc.
  - Datos: cualquier dato en forma electrónica
  - Servicios: cualquier servicio de almacenamiento/tratamiento/comunicación de datos electrónicos
- Resultados indeseables – definidos en términos de la “CIA”
  - Confidencialidad de datos
  - Integridad de datos, sistemas y servicios
  - Disponibilidad (*Availability*) de datos y servicios

Ciberseguridad – Ámbito típico

- Actores de riesgo principales
  1. Actor malintencionado externo (acceso no autorizado)
  2. Amenaza interna (abuso informático)
- Etapas del escenario típico (amenaza externa)
  1. Identificación y reconocimiento del blanco
  2. Penetración
     - Piratería informática
     - Ingeniería social
  3. Explotación
     - Alcanzar el objetivo final del ataque
     - Resultado indeseable para el propietario del bien informático

Tecnología de información (y comunicación) (TI o TCI)

- Hardware
  - “Clientes”: ordenadores portátiles y de mesa, teléfonos inteligentes y tabletas
  - Servidores
  - Equipos de red: conmutadores (switch), routers, aparatos de red (*network appliances*), etc.
  - Nube informática (*Cloud*)
- Software
  - Sistemas de explotación estándares (Windows/Linux)
  - Suites de ofimática
  - Correo electrónico
  - Aplicaciones Web
- “*Todos los utilizan, todos los fabrican …*”

Amenazas cíber dominantes en TI tradicional

1. Cibercrimen de masas
   - Actor de amenaza
     - Grupos internacionales de cibercrimen organizado
   - Vulnerabilidades/Modus operandi
     - Bugs de software bugs explotables en sistemas de explotación y software común
     - Técnicas de ingeniería social
       - Campañas de phishing no dirigidas
       - Optimización ilícita de motores de búsqueda (“Black” SEO)
   - Monetización
     - Fraude publicitario en Internet
     - Fraude bancario y de tarjetas de crédito
     - **Ransomware**
     - Minería de criptomonedas
   - Impacto
     - Financiero: Ninguno a medio
     - Operacional (*ransomware*): medio a severo

Amenazas cíber dominantes en TI tradicional

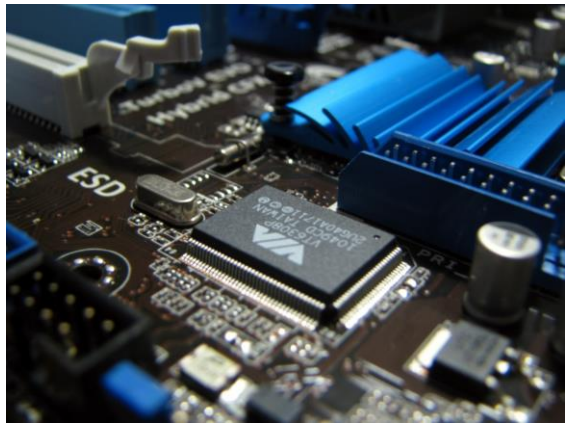
2. Cíber sabotaje (cíber conflictos/guerra)
   - Actor de amenaza
     - Grupos subversivos y “hacktivistas”
     - Actores estatales
   - Vulnerabilidades/Modus operandi
     - Bugs de software bugs explotables en sistemas de explotación y software **específicos**
     - Técnicas de ingeniería social **dirigidas** (harponeo o *spear phishing*)
     - Atatques de cadena de suministro (en mayoría software)
   - Explotación
     - Robo y exposición de información confidencial
     - Indisponibilidad de servicios prolongada (manipulación de configuraciones, encriptatción de datos, “ladrillaje”, etc.)
     - Situación embarazosa deliberada (Página Web vandalizada, publicación de información confidencial, etc.)
   - Impacto
     - Grave a severo

Amenazas ciber dominantes en TI tradicional

3. Amenazas a la cadena de suministro ciber (TI)

Hardware

- Microchips y producción asimétrica de PCB (Asia)
- Bloomberg y Bloomberg 2.0
- Router Wavelink/Jetstream



Software

- Solar Winds
- Telvent

solarwinds

¿Qué hay del riesgo de ataque sobre la cadena de suministro cíber en el ámbito marítimo?

Sistemas ciber físicos (CPS)

- Término genérico para sistemas que :
  1. Tienen una componente cíber (ordenador, lógica programable, etc.)
     Y
  2. *Interactúan* con el mundo físico (sensores & actuadores)
- Incluye
  - Tecnología operacional (TO, OT en inglés)
  - Sistemas de control industrial (ICS)
  - Internet de objetos (IoT)
  - CPS específicos a un dominio
    - Salud y medicina : e.g. desfibriladores cardíacos, bomas de insulina, irradiadores, etc.
    - Aviación: aviónica, Comunicación/navegación/vigilancia (CNS)

ICS genéricos/Tecnología operacional (TO)

- Hardware
  - Sensores and actuadores
  - Controladores de lógica programable (*Programmable logic controllers* - PLC)
  - IT tradicional (laptops/desktops, tabletas, servidores, routers)
- Software y TI de soporte
  - Comunicaciones (redes)
  - Interfaz hombre-máquina & vigilancia a distancia
  - Funciones corporativas (historiadora, facturación, conformidad, etc.)
- Mercado dominado por las “siete hermanas” de los ICS
  - Siemens, Rockwell, Mitsubishi, Schneider Electric, ABB, Honeywell, Hitachi

Otras tecnologías y tendencias notables

- Internet de objetos (IoT)
  - Permitido por la “democratización” de Internet
    - IPv6 – direcciones IP fijas para **todos** y **todo** (every**one** and every**thing**)
    - 5G/Starlink – conectividad IP bajo coste en **todas partes** (every**where**)
- Internet de objetos industrial (IIoT)
  - Democratización en curso de los ICS tradicionales
  - Utiliza la conectividad IP connectivity (p.ej. wifi) como flujo alternativo de datos
  - Permite nuevas aplicaciones de bajo coste por fornecedores no tradicionales
  - Ejemplos
    - Acelerómetros de precisión en fresadoras con conectividad Wifi
    - Raspberry Pi + radio definida por software (SDN) ➔ Flight Aware
- *“¡Todos pueden hacerlo!”*

Amenazas dominantes sobre CPS genéricos (OT/IoT/IIoT)

1. Cíber sabotaje
    - Actor de amenaza
        - Actores estatales
    - Vulnerabilidades/Modus operandi
        - Bugs de software explotables en **software de CPS**
        - Técnicas de ingeniería social **dirigidas** (*spear phishing*)
        - Operativos **combinados**
            - Operaciones especiales
            - Inteligencia física/ciber/técnica/humana
        - Ataques de cadena de suministro
    - Explotación
        - Disrupción de operaciones
        - Indisponibilidad prolongada de servicio (manipulación de configuraciones, encriptación de datos, ladrillage, etc.)
        - Proyección de fuerza (intimidación)
    - Impacto
        - Grave a severo

TI y TO en el ámbito marítimo

	Flete	Puertos	Ayudas a la navegación	Navíos
TI tradicional	- Redes informáticas (IP, Wifi, redes cableadas) - E-mail - Gestión documental y bases de datos - Aplicaciones Web - Pagos electrónicos			

TI específico	- Seguimiento de navíos
	- Seguimiento de flete
	  - Manifiestos
	  - RFID
	  - *Blockchain*
		- Planificación
		- Control de camiones
			- Vessel Traffic Services (VTS)	- Actualización cartas navegación
				- Internet pasajeros/ tripulación

CPS	- RFID - AIS	- RFID - Control de acceso físico - Vigilancia	- Marcas y faros - Boyas - Balizas radar - AIS AtoN - Radar de vigilancia - …	- IPMS - ECDIS - AIS - Radar - Sonar - …

Riesgos potenciales en ciberseguridad marítima

Impacto potencial	***Cui bono* (quien beneficia)**
• Disrupción de flete marítimo (largo plazo) con impacto económico severo	• Actores estatales • Grupos subversivos
• Destrucción catastrófica (incidente marítimo: enbarracamiento, choque)	• Grupos terroristas • Actores estatales
• Disrupción de operaciones de vigilancia marítima (corto plazo)	Crimen organizado • Contrabando/narcotráfico • Migración ilegal/tráfico humano • Cibercrimen (extorsión)

Vulnerabilidades en AtoN/VTS

- “Conocidos conocidos”
  - Falsas señales (*signal spoofing*)
    - AIS
    - Balizas radar
    - Posibles con radios definidas por software (SDR)
      - Fácilmente adquiridas
      - Baratas (50-1000$)
  - Falsa información
    - AIS basados en la Web
- “Conocidos desconocidos”
  - Vulnerabilidades de Software
    - Software VTS
    - Software TI de soporte (navegadores y servidores Web, etc.)
    - Ataques de cadena de suministro (malware)
  - Vulnerabilidades Hardware
    - Contraseñas y configuraciones por defecto
    - Interfaz de gestión a distancia
    - Ataques de cadena de suministro
      - Herramientas de acceso a distancia (RAT) imbricadas en el hardware
      - Interrupción de servicios

Potenciales escenarios de ciberataque marítimo

1. Falsificación de señales AIS y radar
   - Equipo necesario (10-12x)
     - Radios definidos por software (SDN)
     - Nano-ordenadores con capacidad LTE/5G (p.ek. Raspberry PI, Arduino)
     - Drones
   - Modus operandi
     - Transmitir falsos informes AIS y retornos de balizas radar a partir de la costa y SDN montados en drones
     - Comando y control a través de Nano-ordenadores con LTE/5G
     - Evitar triangulación con movimiento y transmisión intermitente
   - Coste
     - 10-30 k$ (equipo)
   - Capacidad técnica necesaria
     - Baja a media
   - Impacto
     - Disrupción a corto y medio plazo de VTS y AtoN (horas a días)

Potenciales escenarios de ciberataque marítimo

2. Pirateo de equipo AtoN
   - Requisitos
     - Conocimiento profundo de sistemas instalados (COTS)
     - Acceso a exploits para vulnerabilidades no corregidas (sin patch)
   - Modus operandi
     1. Aprovechar vulnerabilidades en
        - Arquitectura o software de administración remota de AtoN
        - Errores en configuración de software o de redes
     2. Poner el equipo AtoN en un estado irrecuperable (“ladrillaje”) O
     3. Instalar firmware malévolo en el hardware AtoN para que
        - Actúe de manera no confiable (fallos aleatorios)
        - Mandar información poco fiable o falsa
   - Coste
     - Mano de obra sólo (meses de preparación)
   - Capacidad técnica necesaria
     - Alta
   - Impacto
     - Fuerza el remplazo de componentes físicas
     - Disrupciones a las operaciones de medio o largo plazo (dependiendo de la agilidad de la cadena de suministro)

Retos inherentes a la ciberseguridad marítima

1. Las “tres soledades”
   a. Personal de ciberseguridad y seguridad TI
      - Profesionales internos formados en ciberseguridad genérica de TI
      - Proveedor de servicios de ciberseguridad (consultores, MSSP, etc.)
      - Proveedor de soluciones de ciberseguridad
   b. Especialistas en AtoN/VTS
      - Ingenieros/técnicos internos
      - Fabricantes y proveedores de soluciones AtoN/VTS
   c. Operadores marítimos
      a. Capitanía de puerto
      b. Guardia costera y marina de guerra
      c. Pilotos y tripulaciones

➔ ¿¿Lenguaje común??

➔ Escasez de pericia multidisciplinaria, específica al ámbito marítimo (¿Cómo generarla?)

Retos inherentes a la ciberseguridad marítima

2. Sobre énfasis en “desconocidos conocidos”
   - p.ej. Ciberataques TI, ransomware
   - Cibercriminales atacando infraestructura crítica cada vez más
   - “Zona de confort” de la mayoría de profesionales y organizaciones de ciberseguridad
     - Riesgos conocidos
     - Soluciones y enfoques conocidos (el fenómeno “IBM”)
   - Defensas no consideran y no protegen contra
     - Ataques específicos al ámbito
     - Atacantes más sofisticados y no motivados por el lucro
     - Impactos más severos, generalizados y de impacto duradero (p.ej. Impacto económico a nivel nacional)

Retos inherentes a la ciberseguridad marítima

3. Ignorancia de los eventos de “Cisne Negro” (“desconocidos desconocidos”)
   - Ausencia de ciberataques contra AtoN/VTS (hasta hoy)
   - Poca atención a potenciales eventos/escenarios catástrofes
   - Probabilidad difícil de predecir (por lo baja)
   - Pocos métodos conocidos para detectar y prevenir
   - Falacia del retorno sobre inversión
     - “Demasiado caro” de parar vs. Reducción de riesgo percibida
   - Incentivos personales y organizacionales mal alineados

Conclusiones

- Ciber riesgos más importantes
  1. Ransomware
     - Crimen organizado atacando específicamente infraestructura crítica (sin ser específica al ámbito marítimo)
  2. Falsificación de señales AIS/Radar
     - Por actores estatales o subversivos, causando interrupciones de corto y medio plazo al transporte marítimo
  3. Pirateo de sistemas AtoN
     - Actores estatales o criminales, causando interrupciones de medio y largo plazo al transporte marítimo

Conclusiones

- Prioridades
  1. Adopción rápida e introducción de tecnologías seguras
     - **¡¡¡ AIS seguro !!!**
  2. Estándares de ciberseguridad para productos AtoN y VTS
  3. Factores humanos
     - Vector más importante (pero no único) para el ransomware
     - Cómo gestionar eventos y recuperarse (preparación a las urgencias y continuidad de negocios)
  4. Alcanzar madurez en ciberseguridad genérica TI en la organización
     - A través el espectro completo de funciones de ciberseguridad (marco del NIST)
  5. Desarrollo de soluciones de ciberseguridad al ámbito marítimo