Anatomy of a Cyber Attack

Tactics and techniques span the spectrum of desired outcomes, approaches, and methods

External			Internal			End Goal
	Target Reconnaissance	Gain Access	Establish Command and Control	Persistence	Lateral Movement & Target Access	Execute
	Social Media Use LinkedIn to identify employees who can be targeted as a means to achieving end goal (e.g. system administrator, payroll, accounts payable)	Infect the Target Get employee to click on email attachment or website resulting in installation of malware that allows remote access.	Encrypt Traffic Utilizes encrypted web traffic to send data to and from a compromised computer	Avoid Detection Utilize malicious code that is not easily identified by anti virus software	Compromise Credentials Obtain other valid user IDs / passwords that can use to login to other systems	Exfiltrate Data Gaining access to a server or database storing Client trade positions

Construct a threat taxonomy and detection/prevention from perspective of cyber actor

Maritime Risk Symposium

Targets, Tactics, and Casualties

Highest yielding assets, most impactful systems

Targeted Assets

- Personally Identifiable Information (PII)
- Credit / Debit Card Numbers
- Knowledge Base Authentication (KBA) data
- Material Non-public Information

Methods of Attack

- Aggregate data in dormant storage areas and near to egress points
- Exfiltration through encrypted channels (sftp, https) to help avoid detection
- Malware that encrypts and exfiltrates via outdated protocols (e.g. FTP, SMP)

Notable Attacks / Losses

- Cap One: 100mn ppl ~\$250mn
- Target: 110mn ppl \$300mn
- Marriott: 383mn ppl \$400mn
- Equifax: 147mn people \$1.5Bn
- Sony: digital content PII emails

BUSINESS DISRUPTION

Targeted Systems

- External facing websites
- Internal applications and data
- Vendors (esp. cloud services / storage)
- Domain Naming Services (e.g. Akamai, DYN)

Methods of Attack

- Distributed Denial of Service (DDoS) attack that flood websites w. bad traffic
- Ransomware that encrypts hard drives
- Data deletion / corruption
- Low level format hard disk formats
- > GPS Spoofing and Jamming

Notable Attacks / Losses

- 2012 Saudi Aramco: 2 month disrupt.
- 2016 DYN: 2 hour internet disruption
- > 2017 NotPetya: ~\$10bn losses
- > 2019 AWS Route 53: 8 hour disruption
- 2017 ~ 2019 various GPS spoofs

PAYMENT FRAUD

Targeted Systems

- Internal Payment Processing Systems (e.g. account payable, wire transfers)
- Central Payment Routing Systems (e.g. SWIFT, SPEI)
- Business Email Compromise (BEC)

Methods of Attack

- Remote Access Trojan (RAT) to take over employee's user account and all of their internal systems access
- Exploit vulnerabilities in proprietary and third party software
- Phishing and impersonation emails to divert payments and payrolls

Notable Attacks / Losses

- Bank of Bangladesh SWIFT: \$81mn
- Cosmos Bank Payments: \$13.5mn
- Mexico SPEI: \$15.2mn
- Nikkei BEC: \$29mn
- Toyota Boshoku BEC: \$37mn

Maritime Risk Symposium

Challenges and Inter-dependencies

Challenges to All Industries Constantly evolving adversaries and tactics Weakest links - Clients - Vendors - Supply-chain - Business Email Compromises (BEC) Day zero vulnerabilities with known exploits End of Life Software - Operating Systems - Web infrastructure - Software libraries Laws and Regulations - variances by state / country - fines based on revenue (e.g. GDPR)

2018 Global Bank Shipping Portfolios(\$Bn)



Maritime Risk Symposium

Success Stories

Self Defense

- Multifactor authentication
 - external-facing portals
 - sensitive internal applications
- Virtualization
 - VPNs
 - Citrix applications

Hygiene

- Patching
- End of Life / End of Service

Specialist Teams

- Threat Intelligence
- Vulnerability Management
- Incident Response Center
- Hunter
- Fusion

Financial Services Cooperation

Industry Consortiums

- FS-ISAC incident & vulnblt'y share
- FS-ARC stress & resiliency testing
- FSSCC DHS coordination
- FBIIC US Treasury coordination
- ORX anonymized incident share
- Industry Exercises / Frameworks
 - NIST Cybersecurity Framework
 - SIFMA Quantum Dawn
 - Bank of England CBEST
 - MITRE ATT&CK
 - FS-IASC CAPS
 - HKMA CRAF
- SWIFT Out of band Reconciliation