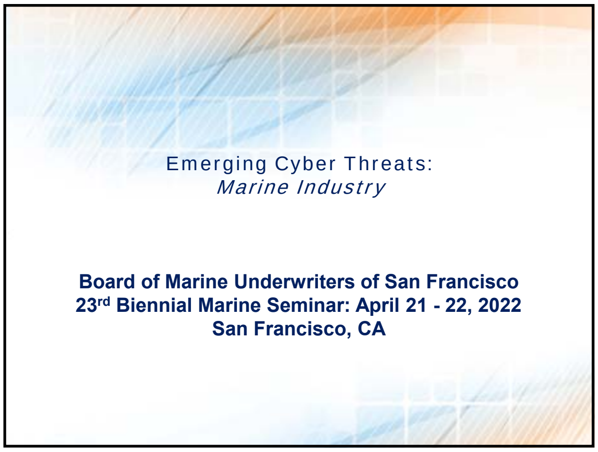
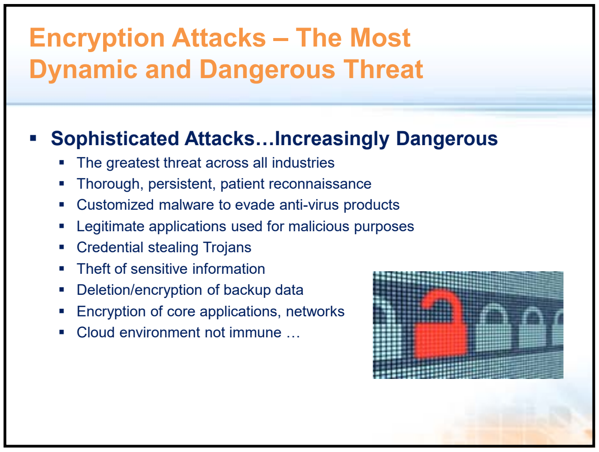


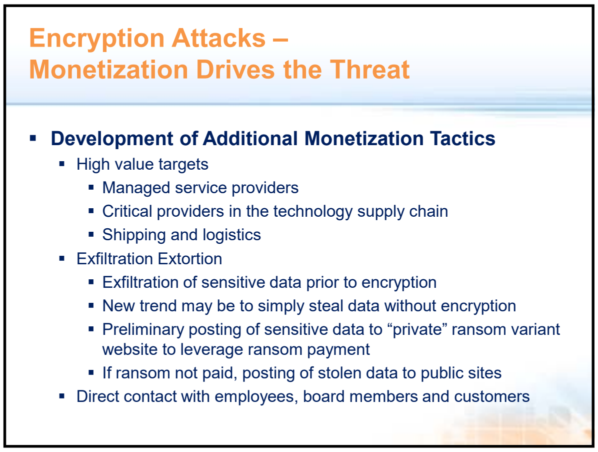
Emerging Cyber Threats: *Marine Industry*

Board of Marine Underwriters of San Francisco
23rd Biennial Marine Seminar: April 21 - 22, 2022
San Francisco, CA



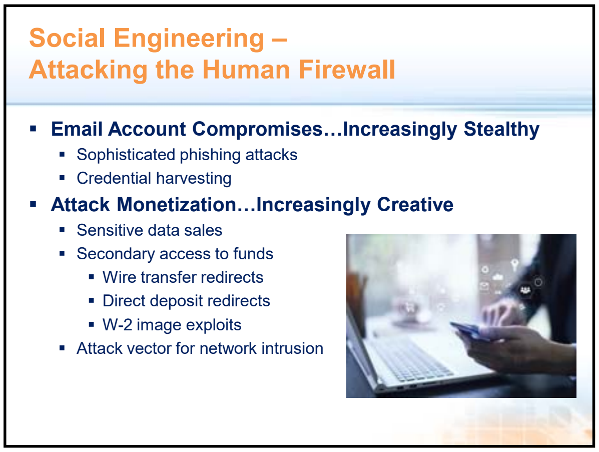
Encryption Attacks – The Most Dynamic and Dangerous Threat

- **Sophisticated Attacks…Increasingly Dangerous**
  - The greatest threat across all industries
  - Thorough, persistent, patient reconnaissance
  - Customized malware to evade anti-virus products
  - Legitimate applications used for malicious purposes
  - Credential stealing Trojans
  - Theft of sensitive information
  - Deletion/encryption of backup data
  - Encryption of core applications, networks
  - Cloud environment not immune …



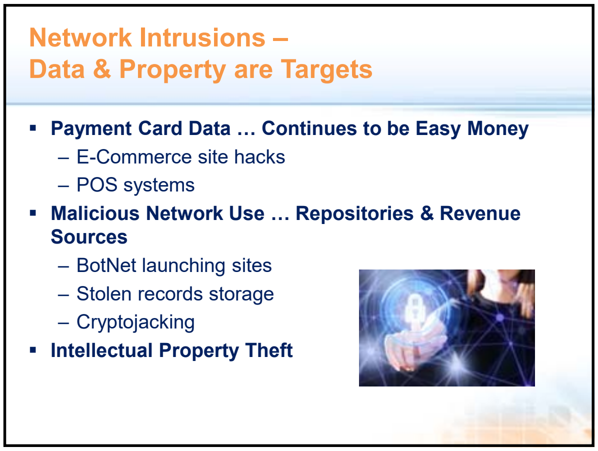
Encryption Attacks – Monetization Drives the Threat

- **Development of Additional Monetization Tactics**
  - High value targets
    - Managed service providers
    - Critical providers in the technology supply chain
    - Shipping and logistics
  - Exfiltration Extortion
    - Exfiltration of sensitive data prior to encryption
    - New trend may be to simply steal data without encryption
    - Preliminary posting of sensitive data to “private” ransom variant website to leverage ransom payment
    - If ransom not paid, posting of stolen data to public sites
  - Direct contact with employees, board members and customers



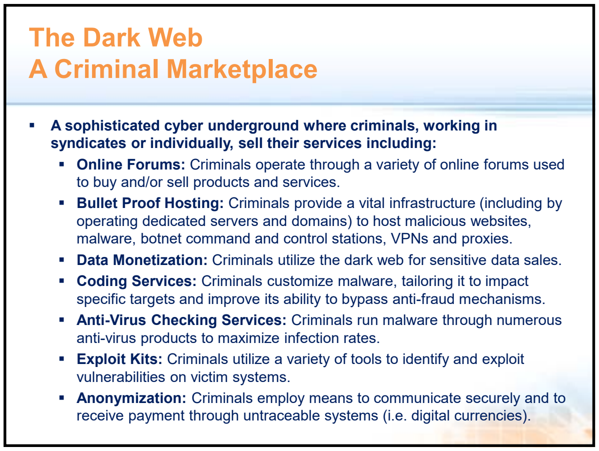
Social Engineering – Attacking the Human Firewall

- **Email Account Compromises…Increasingly Stealthy**
  - Sophisticated phishing attacks
  - Credential harvesting
- **Attack Monetization…Increasingly Creative**
  - Sensitive data sales
  - Secondary access to funds
    - Wire transfer redirects
    - Direct deposit redirects
    - W-2 image exploits
  - Attack vector for network intrusion



Network Intrusions – Data & Property are Targets

- **Payment Card Data … Continues to be Easy Money**
  – E-Commerce site hacks
  – POS systems
- **Malicious Network Use … Repositories & Revenue Sources**
  – BotNet launching sites
  – Stolen records storage
  – Cryptojacking
- **Intellectual Property Theft**



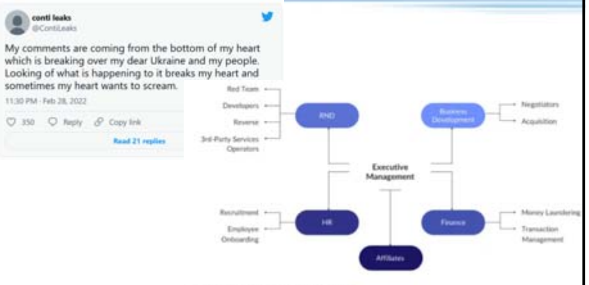
The Dark Web A Criminal Marketplace

- **A sophisticated cyber underground where criminals, working in syndicates or individually, sell their services including:**
  - **Online Forums:** Criminals operate through a variety of online forums used to buy and/or sell products and services.
  - **Bullet Proof Hosting:** Criminals provide a vital infrastructure (including by operating dedicated servers and domains) to host malicious websites, malware, botnet command and control stations, VPNs and proxies.
  - **Data Monetization:** Criminals utilize the dark web for sensitive data sales.
  - **Coding Services:** Criminals customize malware, tailoring it to impact specific targets and improve its ability to bypass anti-fraud mechanisms.
  - **Anti-Virus Checking Services:** Criminals run malware through numerous anti-virus products to maximize infection rates.
  - **Exploit Kits:** Criminals utilize a variety of tools to identify and exploit vulnerabilities on victim systems.
  - **Anonymization:** Criminals employ means to communicate securely and to receive payment through untraceable systems (i.e. digital currencies).

Conti Ransomware Group Leaks

- In February of 2022, leaked documents provided significant insight into the internal operations of *Conti* – one of most notorious ransomware groups
- *Conti* operates as a ransomware-as-a-service (RaaS) model ransomware variant
- A massive, structured organization with internal "departments":
  - Executive management
  - HR and recruiting
  - Research and development
  - Finance

Conti Ransomware Group Leaks



conti leaks
@ContiLeaks

My comments are coming from the bottom of my heart which is breaking over my dear Ukraine and my people. Looking of what is happening to it breaks my heart and sometimes my heart wants to scream.

11:30 PM · Feb 28, 2022

Figure 8: Conti's organization chart concluded from the leaks

Source: Cyberint

The Regulatory Environment – A Reason for a Sense of Urgency

- **State Data Breach Notification Statutes**
- **Self-funded operations budgets - funded by assessments …**
  - **All 50 states** plus Washington D.C., Guam, Puerto Rico, and Virgin Islands
  - **All cover electronic**, 10 also cover paper;
  - **Require notification of consumers** regarding breaches of unencrypted personal information;
  - **Notification** obligation **determined by residential location of consumer**, not location of business
  - **Personal information** generally defined as first name or initial and last name, combined with one or more of the following data sets:
    - All states include SSN, DL or State ID card number, or financial account with means to access the account;
    - 19 add medical information; 18 add health insurance; 18 add biometric information; 18 add online credentials; etc.

The Regulatory Environment – A Reason for a Sense of Urgency

- **State Data Breach Notification Statutes (continued)**
  - **Timing of notification**: 40 require "most expedient time possible;" 18 also have outer time limit (ranging from 30 to 90 days);
  - **Notice content requirements**: 19 have specific notice content requirements;
  - **Regulatory notification**: 35 require notification of state regulatory officials;
- **State Data Privacy Legislation**
  - **California Consumer Privacy Act**
    - Affords consumers private right of action arising from unauthorized disclosure of personal information
- **State Information Security Standards**
  - Triggered by **Unfair Trade Practice Acts**
- **Federal Sector Regulations**
  - **HIPAA**
- **Industry requirements**
  - **PCI DSS**

Most Troubling Trends

- **Targets**: Increasingly high value (MSPs, supply chain, certain sectors/verticals), but entities in all locations, in all industries, and of all sizes remain targets
- **Sophistication**: Attacks increasingly sophisticated, substantial reconnaissance
  - Encryption extortion: Deletion of backup data, encryption of core applications
  - Exfiltration extortion: Increasing ransom demands, theft of sensitive data
  - Social engineering: Increasingly difficult to detect
- **Frequency:** Entities are targeted daily by social engineering and brute force attacks
- **Success**: Increasingly successful encryption attacks with decreasingly ability to negotiate ransom demand
- **Regulatory Action**: Increasingly aggressive state regulatory agencies

High Value Targets

- Maritime services companies have increasingly become targets
  - Perceived as having ability to pay large ransoms
  - Especially sensitive to downtime
  - Necessary possession of sensitive information
  - Increased reliance on technology = greater attack surface
- Supported by the security research data:
  - Ransomware attacks experienced by shipping and logistics companies tripled from 2019 to 2020.
  - The world's four largest maritime shipping companies were all victims of ransomware attacks since 2017.
- Federal government recommendations for maritime cybersecurity

Cyber Insurance and Response

- The Cyber Insurance Market
- Notice Provisions
- Insuring Agreements

Cyber Insurance and Response

- Typical First-Party Coverages
  - Incident Consultation / Legal
  - Forensics
  - Extortion
  - Notification
  - Data and System Restoration
  - Crisis Management
  - Business Interruption and Contingent Business Interruption
  - Cyber Crime Coverage

Cyber Insurance and Response

- Typical Third-Party Coverages
  - Defense Expenses
  - Network Security Incident and Privacy Incident Liability
  - Media Incident Liability
  - Regulatory Costs
  - PCI Costs

Cyber Insurance and Response

- Incident Response Panels
  - Breach Coach
  - Forensics
  - Data Mining
  - Restoration
  - Notification
  - Crisis Management