Who Am I?

- Over 20 years experience with 17 years in the financial industry in Information Security Management, Risk Management, Third Party Oversight and Integrated Auditing.
- Presented security, vendor management and IT audit topics in such forums as the 2014 IIA/ISACA Governance, Risk and Controls Conference, 2013 ISACA Chapter Leadership, 2011-2013 University of North Florida Cybersecurity forums and 2012-2015 IT Pro-Camps.
- CISA, CISM, CRISC, CRMA
- Adjunct Professor with ITT-Tech with over 5 years teaching.
- Chapter President for the ISACA Jacksonville Chapter.
Agenda

- Introduction
- Advanced Persistent Threats
- Cybersecurity Kill Chain
  - Lockheed Martin
  - ISACA Cybersecurity Nexus
  - European Union Agency for Network and Information Security
- Summary
- Questions
Introduction

Based off military doctrine, Lockheed Martin’s Computer Incident Response Team has created an intelligence-driven defense process, Cyber Kill Chain® allowing cyber security professionals to proactively remediate and mitigate advanced threats. To be successful against a new class of threats, appropriately dubbed the “Advanced Persistent Threat” (APT), representing well-resourced and trained adversaries conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information defend like an attacker; apply the Cyber Kill Chain®
Advanced Persistent Threats

- An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

- These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.

- The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders’ efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.
Advanced Persistent Threats

- APTs are advanced and stealthy, often possessing the ability to conceal themselves within the enterprise network traffic, interacting just enough to get what they need to accomplish their job. This ability to disguise themselves and morph when needed can be crippling to security professionals’ attempts to identify or stop APT attacks.
Lockheed Martin Cybersecurity Kill Chain

- **Reconnaissance**
  - Harvesting e-mail address, conference information, Social Engineering

- **Weaponization**
  - Compiling exploit with backdoor into delivery payload

- **Delivery**
  - Delivering weaponized bundle to the victim via e-mail, USB, web

- **Exploitation**
  - Exploiting a vulnerability to execute code on a victim's system
Lockheed Martin Cybersecurity Kill Chain

- Installation
  - Installing malware on the asset
- Command and Control (C2)
  - Command channel for remote manipulation of victim
- Action on Objectives
  - Hands on access to asset allows intruder to attain goals
Perform reconnaissance:
- The adversary gathers information using a variety of techniques

Create attack tools:
- The adversary crafts the tools needed to carry out a future attack

Deliver malicious capabilities:
- The adversary inserts or installs whatever is needed to carry out the attack

Exploit and compromise:
- The adversary takes advantage of information and systems in order to compromise them
ISACA Cybersecurity Nexus

- **Conduct an attack**
  - The adversary coordinates attack tools or performs activities that interfere with organizational functions.

- **Achieve results**
  - The adversary causes an adverse impact

- **Maintain a presence or set of capabilities**
  - The adversary continues to exploit and compromise the system]

- **Coordinate a campaign**
  - The adversary coordinates a campaign against the organization
European Union Agency for Network and Information Security
Cybersecurity Kill Chain

- **Reconnaissance:** Identity Theft /Fraud, DOS, Phishing, Spam
  - The action of researching and analyzing information about the target and the environment within which the attack will be deployed. In this phase, assumptions for the number and kind of vulnerabilities to be exploited are being made.

- **Weaponization:** Drive-by Downloads, Exploit Kits, Identity Theft, Fraud, DOS, Phishing, Spam
  - The phase where the malicious payload to be used has been selected and “loaded”, that is, made ready for use for the target environment.

- **Delivery:** Drive-by Downloads, Exploit Kits, Identity Theft /Fraud, DOS, Phishing, Spam
  - The action of transmission of the malicious payload to the target environment.
European Union Agency for Network and Information Security
Cybersecurity Kill Chain

- **Exploitation**: Code Injection, Drive-by Downloads, Exploit Kits, Identity Theft
  Fraud,DOS
  - The act of letting the delivered payload make his job by exploiting vulnerabilities that are available in the target environment. Usually these are technical vulnerabilities but in some attacks these may well also be systemic or organizational vulnerabilities including humans.

- **Installation**: Code Injection, Worms/Trojans, Exploit Kits, Identity Theft
  /Fraud,DOS
  - The phase where the delivered payload has successfully exploited a vulnerability and has been installed in the target environment.

- **Command and Control (C2)**: Trojans, Botnets,DOS
  - The installed payload establishes outbound connection to the controller environment in order to enable interaction with the adversary who launched the attack.
Action on Objectives: Physical Damage/Theft/Loss, DOS

This is the final phase of a successful attack where the threat agent is in the position to take over the targeted asset. Depending on the kind of target, this activity may include information retrieval, information manipulation, application misuse, etc.
Summary

- Cybersecurity Kill Chain
  - Lockheed Martin
  - ISACA Cybersecurity Nexus
  - European Union Agency for Network and Information Security
References

- ISACA, CSX Cybersecurity Fundamentals, 2014 Study Guide
- ISACA, Advanced Persistent Threats: How to Manage the Risk to your Business, 2013
- ENISA Threat Landscape 2013 -*Overview of current and emerging cyber-threats* -11 December 2013
- Lockheed Martin-Cyber Kill Chain®
Questions