Prepare Yourself for the Digital Battlefield

Christopher May

27 Feb 2014
Overview

Who... is this guy?

What... is the Digital Battlefield?

Why... do I want to work in Cyber Security?

How... can I prepare myself?
  • Careers
  • Tactics and Tools
  • Gain Experience

Demos

Case study

Questions
Who is this guy?

Advance Cyber Tradecraft of

- CERT/SEI = DoD Federal Lab
- Cyber Workforce Development

Professor

- INI’s CyFIR Track, AIA, IACBP

Researcher

- APT, COPs, Mod/Sim, SCADA, Cyber Intel

Cybersecurity Warrior

- Captain US Air Force

Family Man, Volleyball Coach, Sailor… 😊
What is the Digital Battlefield?

It’s the Internet and way beyond…

Persistent global conflict

- Borderless and Faceless
- Waged by criminals/nations for profit and power

Bad Guys:

- Always maintain tactical advantage
  - Near complete freedom of maneuver
    - Maginot vs. Blitzkrieg
- Cheap weapons = massive damage (and easy $)

Good Guys:

- Constrained by rule of law = perpetually defensive
  - Security is a cost center
Why do I want to work in Cyber Security?

Cool Jobs and Lots of them!

“The U.S. Bureau of Labour Statistics says the number of Information Technology security roles in the U.S. will increase by some 22 percent in the decade to 2020, creating 65,700 new jobs. Experts say it is a similar situation globally, with salaries often rising 5-7 percent a year.”

Citizen Soldiers?

• You get to be one of the Good Guys
• But sorry…No cool Uniforms！ 😞
How can I prepare myself?

You Must Know **What** to Learn First !!

**STEP 1:**

- Learn about Cyber Security Careers
  - Know Specialty Areas and Key Tasks
    - Review KSAs

---

**NICCS™**

**NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES**

---

**Official website of the Department of Homeland Security**

---

CERT | Software Engineering Institute | Carnegie Mellon University
How can I prepare myself?

STEP 2:

Establish a Solid Foundation

- Prerequisite knowledge
  - Computer System Fundamentals
    - Components and their properties
      - HDDs, RAM, Peripherals, etc.
  - Computer Networking Fundamentals
    - Protocols: OSI, TCP/IP, and Ethernet
    - Devices and their properties
      - Routers, Switches, Wireless APs, etc.
  - Operating Systems
    - Windows, Linux, OSX, perhaps Cisco IOS
How can I prepare myself?

STEP 3: Join Professional Associations:

Subscribe to and Read Security Blogs Daily!

• Here are a few that I like:
  
  - Krebs on Security
  - Malwarebytes UNPACKED
  - ZDNet
  - dark READING
  - Zero Day
  - naked security
How can I prepare myself?

STEP 4:
Develop Security Skillz w/ Toolz of the Trade

- Virtualization Platforms:
- Host Security:
- Vulnerability Scanning and Testing:
- Network Security Monitoring:

Ancient Wisdom: Knowledge **Must be Applied.**
Practice Daily !!
How can I prepare myself?

STEP 4: (con’t)

Develop **Analysis** Skillz with Toolz of the Trade

- Incident Response and Forensics:
  - Autopsy
  - SANS Investigate Forensic Toolkit (SIFT)

- Malware Analysis:
  - Comodo Instant Malware Analysis
  - Cuckoo
How can I prepare myself?

STEP 5:

Gain Real-World Experience

• Most Challenging Step for Students
  • Internships with Corporate Security Teams
  • Online CTFs and Exercises
  • Use Case Studies.
    • Dissect Large Intrusions by collecting and analyzing Open Source Intelligence
Target Inc. Intrusion Case Study

Quick example of a technique for building experience
Target Questions

Order of events

• What vulnerabilities were exploited? How was important data obtained, exfiltrated, and monetized?

Detection

• How did the organization find out what was happening?

Cost

• Monetary loss or gain for the company, customers, or others?

Threat actor profile

• Number of people/organizations involved?
• Skills required?

Mitigation

• What can be done to prevent, respond more quickly, or minimize losses in the future?
Target Order of Events, with some speculation

1) Attackers *may* have executed a phishing email campaign against one or more employees at Fazio Mechanical, the HVAC vendor for several Target stores.

2) Zeus financial malware variant *Citadel Trojan* infects employee computer at Fazio Mechanical and is used to steal passwords.

3) Attackers *may* have gained access to one or more external Target systems; Ariba used for external billing, Partners Online used for project management, or Target’s Property Development Zone portal.

4) Attackers *may* have been able to pivot from one or more external system into the Target internal network. Perhaps using Active Directory admin credentials available on the external system.

5) BlackPOS malware was loaded onto cash registers. BlackPOS uses a derivative of the the *Trojan.POSRAM* virus. Scrape memory for cc data.

6) Credit card data stored on an internal Windows share before being exfiltrated.

7) Stolen credit card data transferred via FTP to several US “drop” locations, and eventually to servers in Russia.
Cost

Monetary loss or gain for the company, customers, or others?

• 40 million credit card numbers used between Nov 27 and Dec 15
• Personal information for about 110 Million people
• Investigation effort?
• Legal fees, class-action lawsuits, regulatory fees, and other settlement
  • Some estimate $1 Billion
• Decline in stock prices
• Customer credit monitoring
• Indirect costs
  • Customer loyalty & confidence
  • Already cost credit unions as much as $30 million
  • $1.4 billion to $2.2 billion in fraudulent charges
Target Mitigation Summary

What can be done to prevent, respond more quickly, or minimize future losses?

- Defense-in-depth controls
  - Email filtering
  - End-point protection
    - AV, Firewalls, Integrity monitoring
  - User training and awareness
  - Outbound protocol filtering
  - Network segmentation
  - Network ACLs
  - Network IDS/IPS

- Authentication strategy
  - Multi-factor authentication
  - Separate authentication realms

- Allow POS do only POS
- Free and paid-for intelligence monitoring services
- Insider Threat monitoring
- Compliance and Security training for all employees
- Encourage POS switch to Chip and Pin solutions
- Supply Chain Risk Assessment
Questions??