A FRAMEWORK FOR "ADVANCED" NETWORK SECURITY

2018-07-02

Case Study: Advanced Persistent Threat

- Entry
- Recon
- Expand
- Capture/Control
- Extract
- Disappear

Symantec's APT Analysis

- Long-term Planning
- Purposeful Selection of Targets
- Customized Approach (Context)

SANS Analysis of APT-Style Malware

- Social Engineering
- Broad Network Gathering
- Armor Piercing (Anti-Anti Virus)

What does APT teach us about hacking?

- Intelligent
- Patient
- Customized
- Forward Thinking
- *In short, "Advanced"*

Is network security comparable?

- Checklists
- Standard/Generic Tools (typically misconfigured)
- Reactive approaches

Case Study: "What We Did Wrong" Paper

- Recommendation #1: Defense in Depth
- Recommendation #2: Patches
- Recommendation #3: Network Access Control
- Recommendation #4: Traffic Inspection
- Recommendation #5: Host Intrusion Protection System (HIPS)

Personal Dislike: Defense in Depth

- OK if discussing covering all known attack vectors
- However, is often CODE for
  - We don't know what to do, so let's do a lot of it!
  - What we didn't do didn't work, so Let's do a lot of it!

Compare and Contrast Attack/Defense

- The Attackers innovate
- The Defenders Respond

Compare and Contrast Attack/Defense

- The Attackers plan a specific assault
- The Defenders employ a generic defense

Compare and Contrast Attack/Defense

- The Attackers profile users and customize based on target data
- The Defenders use tools that users don't understand, and/or automate

"Advanced Persistent Defense"

- What would a disruptive security approach look like?
- Could it parallel APT?
- What might some analogs be?

EXAMPLE: ADVANCED PERSISTENT DEFENSE

- "Initial Installation" instead of Entry
- "Analysis" instead of Recon
- "Customize" instead of Expand
- "Neutralize" instead of Capture/Control
- "Analyze" instead of Extract
- "Metrics" instead of Disappear

A WORD ABOUT METRICS

- DO YOU KNOW IF YOUR SECURITY "WORKS"?
- HAS IT PREVENTED ANY ATTACKS?
- SEE 4.4 IN LOCKHEED'S "7 WAYS" PAPER

Assignment: Your Vision of APD

- Propose your own framework
- Investigate research/industry sources related to your ideas
- Write a 5 page paper detailing your analysis
- Due February 19th by Start-of-Class