سبر 1213
Network Defense

Lecture #6 Part 2

Comparing Threats, Vulnerabilities, and Common Attacks

Social Engineering

- Impersonating
  - Such as an authorized technician
- Shoulder Surfing
  - Can be in person looking at a computer
  - Can be with a remote camera
- Tricking users with hoaxes

Social Engineering

- Tailgating
  - – Closely following authorized personnel without providing credentials
  - – Mitigated with mantraps

- Dumpster diving
  - – Searching through trash looking for information
  - – Mitigated by shredding or burning papers

Social Engineering

- Zero-day vulnerabilities
  - Unknown to trusted sources, such as operating system and antivirus vendors

- Watering hole attack
  - Attacker identifies websites trusted by group of users
  - Attacker infects these websites
  - Users go to infected (but trusted) websites
  - Prompted to download files

Social Engineering

- Typo squatting (called URL hijacking)
  - Hosting a malicious website
  - Earning ad revenue
  - Reselling the domain

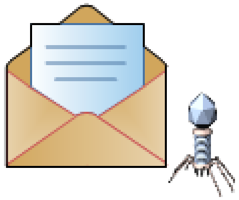
- Elicitation
  - Active listening
  - Reflective questioning
  - False statements
  - Bracketing

Attacks via Email and Phone

- Spam
  - Unwanted or unsolicited email
- Spam over internet messaging (SPIM)
  - Unwanted messages sent over instant messaging (IM) channels
- Phishing
  - Email from friends
  - Installing malware
  - Validating email address
  - Getting money

Attacks via Email and Phone

- Spear Phishing
  - Targeted form of phishing
  - Attempts to target specific groups of users, or even a single user

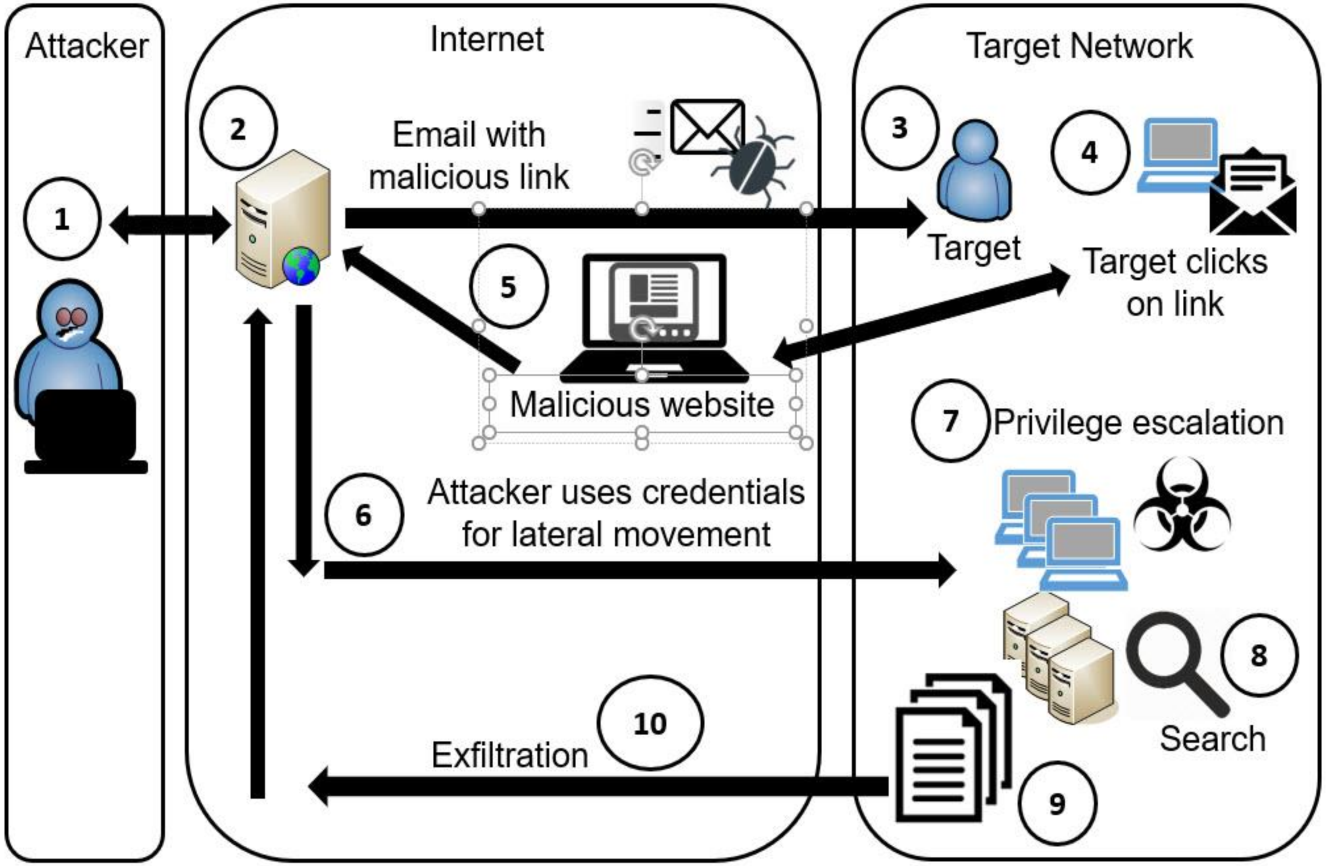


- Whaling
  - Form of spear phishing that attempts to target high-level executives

Attacks via Email and Phone

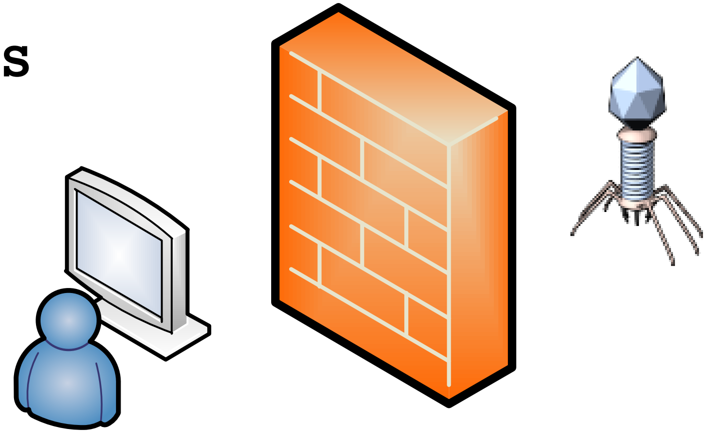
- Vishing
  - use the phone system to trick users
- Smishing
  - a mashup of SMS and phishing
  - uses text instead of email

One Click Lets Them In



Blocking Malware

- Spam filter on mail gateways
- Anti-malware software on mail gateways
- Anti-malware software on all systems
- Block at boundaries
  - Firewalls
  - UTM systems



Blocking Malware

- Antivirus software
  - Signature-based detection
    - Detects known malware based on signature definitions
  - Heuristic-based detection
    - Detects unknown malware based on behavior
  - File integrity monitors
  - Cuckoo sandbox

Why Social Engineering Works

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust

Common Types of OSINT

- Open source intelligence (OSINT)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - Structured Threat Information eXpression (STIX)
  - Public/private information sharing centers
  - Automated indicator sharing (AIS)
  - Indicators of compromise
  - Vulnerability databases
  - File/code repositories
  - Predictive analysis
  - Threat maps

Research Sources

- Vendor
- Conferences
- Academic journals
- Local industry groups
- Request for comments (RFC)
- Public/private information sharing centers
- Social media

Chapter 6 Summary

- Understanding Threat Actors
- Determining Malware Types
- Recognizing Common Attacks
- Blocking Malware and Other Attacks
- Check out the free online resources