Security Architecture
- Week 15 -

Advanced Persistent Threats
Offensive Security

Week 15

- Weekly Assignment Catch-up
- Final Project
- Final Exam
- Lecture: APT/Offensive Security

Weekly Assignment Catch-up

Final Project

- Due by end of day – Saturday April 25th
- pdf format
- Include last name of people on team and Final Project in email subject

Final Exam

- Probably 100 multiple choice
- Bring #2 pencils
- Only 1 right answer
- Up to 20% of questions may come from lecture materials

Advanced Persistent Threats

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes orchestrated to target a specific entity over an extended period.

Modified from Wikipedia

Advanced Persistent Threats

- What is an advanced persistent threat?
- Recent examples
- Detecting APTs
- Responding to APTs
- Architectural protections
- Network architecture approaches
- Emerging market for 3rd party tools

What is an APT?

- Stealthy intrusion
- No disruption of operations
- Often exploit an zero day vulnerability
- May use encryption of malware payload when at rest to avoid signature based detection
- Coordinated communication to a command and control component
- Polymorphic malware
- Use of legitimate IP address destinations
- Careful extrication of captured data to avoid DLP/ log surveillance detection
-

What is an APT?

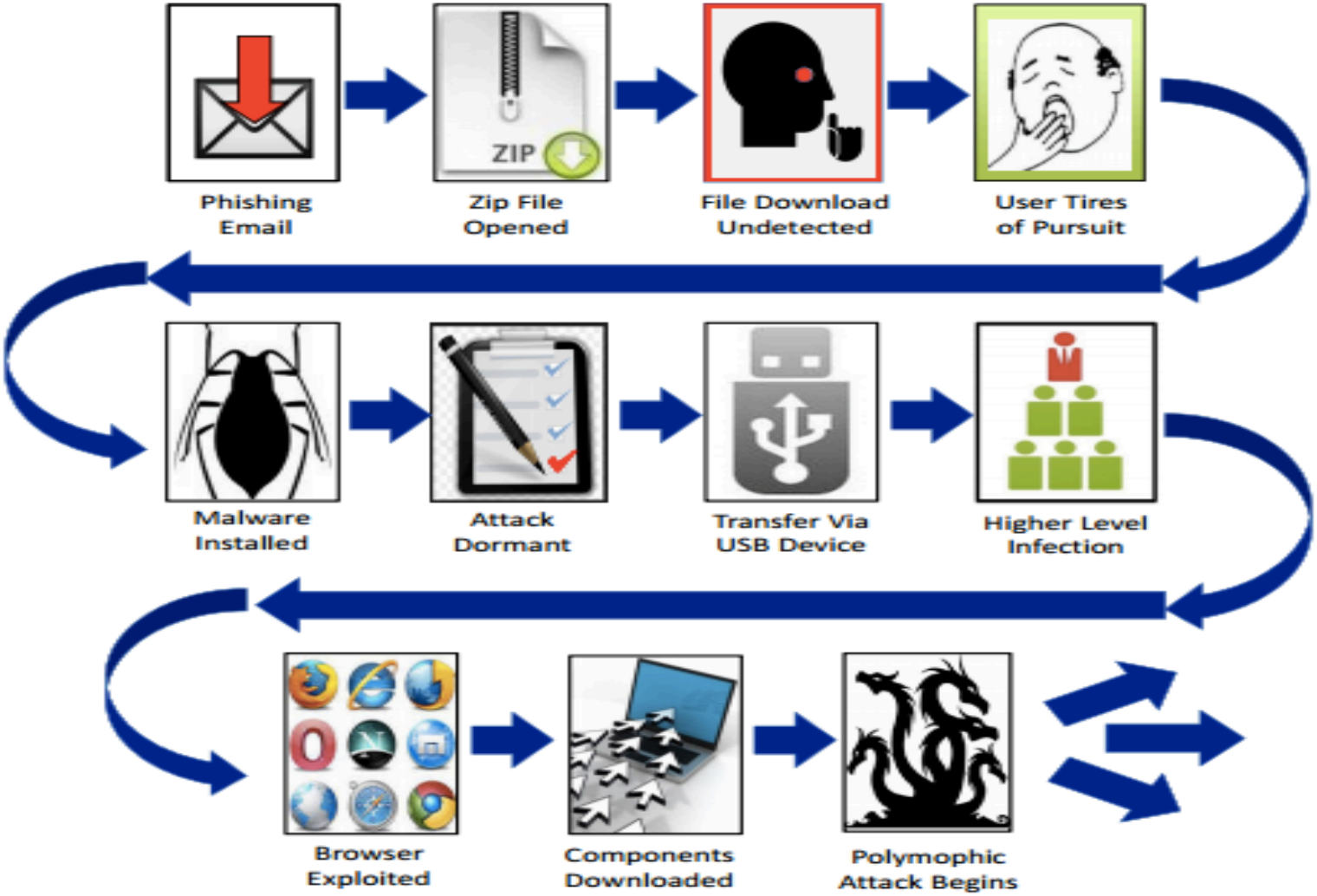

Figure 2: Genesis of an Advanced Persistent Threat

What is an APT?

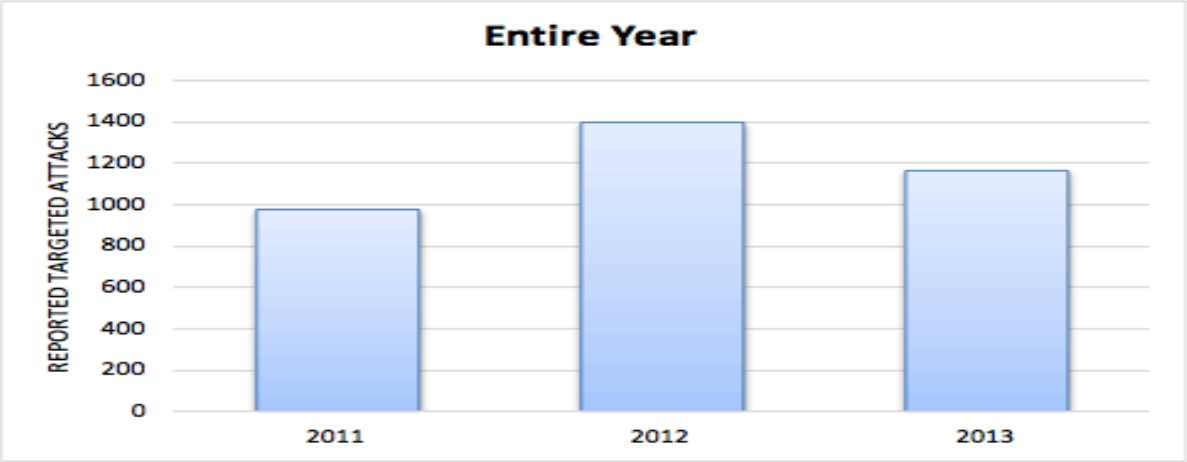

Figure 1: Targeted Attacks in 2013

Recent APT Examples (2014)

- Target
- Home Depot
- Sally Beauty
- Michaels
- Affinity Gaming (11 casinos)
- PFChangs
- UPS
- JPMorgan Chase

Detecting APTs

- Usually discovered substantially after the intrusion
- Indirect evidence like Credit Card numbers for sale on the dark web sometimes are the first indication
- Malware searches sometimes catch a malware component in action and lead to a more thorough investigation
- Log data analysis and network activity tracking are the most common proactive discovery tools

Responding to APTs

- Once discovered curtailing traffic to a command and control system is the typical first step
- Identification of and detection of malware components
- Review of backup and configuration detail to identify the earliest time before the intrusion
- Restoration of systems and data to a “clean” state
- Monitoring of system activities and sometime whitelisting of machines and application services as a means of assuring eradication
- Update to surveillance and detection parameters to avoid re-infection

Responding to APTs

Figure 4: Cyber Security Operations

Architectural Protections Against APTs

- IDS
- DLP
- SIEM
- Security Analytics
- Automated Discovery / Machine Learning

The intersection of ML and IT Security focuses on analytics – an emerging buzzword in security that implies more than just reporting. It encompasses an automated analysis of data that ideally elevates the proverbial needle in the haystack that represents a real threat above the typical noise in the system.*

* Travis Green – Security Week

Network Architecture Approaches

- Sub-netting
- Domain structure
- Hardware selection
- Netware configuration
- Protocol use
- Examples:
  - Sony example
  - Disney
- Why isn't this addressed?
- Who makes the decision? Cost/benefit

3rd Party Tools

- Emerging market for 3rd party tools
- Threat Intelligence as a growing discipline and market opportunity
- Government regulatory-based information sharing
- Popular tools
  - Splunk
  - Fireeye
  - Websense
- In 2014 roughly 1200 new cyber security companies obtained venture funding*

*Peter Clay, the Chief Information Security Officer at Invotas

Offensive Security

Retaliatory actions that extend beyond simply increasing defensive perimeter security measures in response to a cyber attack or even the threat of one

Offensive Security

- What do we mean by offensive security?
- Cyber warfare versus information security
- Government-sponsored Offensive Security
- Commercial Offensive Security
- Japanese example
- Other recent examples
- Ethical and legal considerations
- Architectural underpinnings of offensive security

What do we mean by Offensive Security?

- Not just protection
- Goal: neutralize or disable
- Classic steps
  - Planning
  - Surveillance
  - Analysis
  - Vulnerability Detection
  - Exploitation
  - Active Monitoring

What do we mean by Offensive Security?

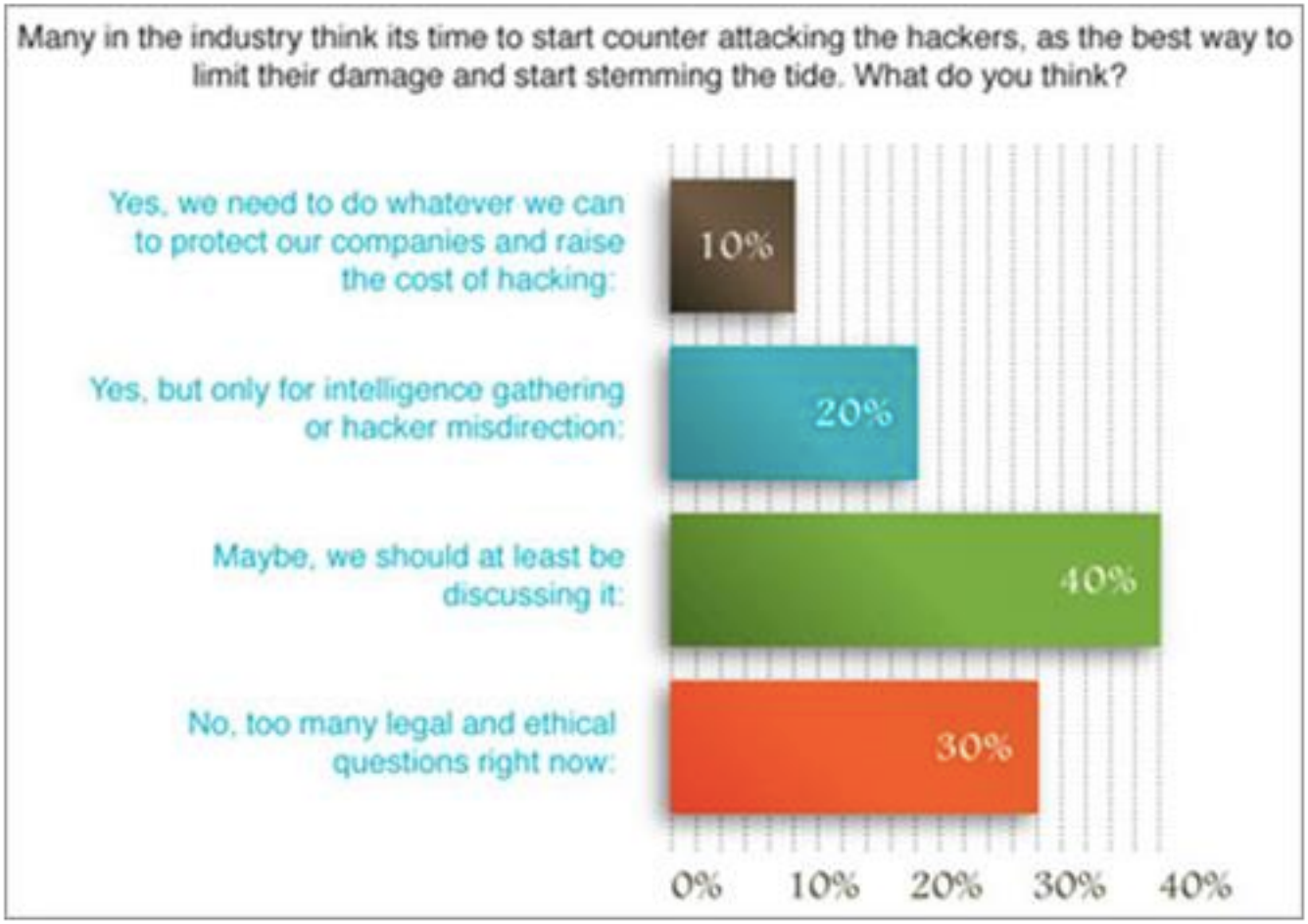

Figure 3 – Offensive approach survey – Wisegate (April 2013)

Cyber Warfare versus Information Security

- Tactics are similar
- Goals and actors vary
- Cyber warfare
  - State sponsorship
  - Large scale
  - Proactive
- Information Security
  - Commercial
  - Smaller attack surface
  - Retaliatory

Government-sponsored Offensive Security

- Most wherewithal for elaborate execution
- Part of national defense
- US is considered by many as the leader in capabilities
- Most countries have some capabilities
- Well know States with offensive capabilities include:
  - China
  - Russia
  - Iran
  - Israel

Japanese Example

- Starting in 2008
- Government sponsored academic research into cyber weapons development
- Government contracted with private companies to develop DDOS-based counter-measures
- Goals:
  - Curtail attacks
  - Disable attackers from executing future attacks

Other Recent Examples

- Mandiant/Google NSA-supported Chinese focused counter-measures
- CrowdStrike takedown of thousands of nodes of the Kelihos botnet
- Crypto-locker counter attack
  - Penetration
  - Data Extraction
  - Distribution of acquired encryption keys

Ethical and Legal Considerations

- Controversial US practice of installing back-doors
- Corporate liability for “collateral damage” and “friendly fire” incidents
- Local laws and restrictions
- Possibility of escalation

Architectural Underpinnings of Offensive Security

- Similar to penetration testing constructs
- Surveillance capabilities
- Analytics tools
- Vulnerability Detection
- Exploitation strategy and tools
  - Botnets
  - Zero day exploits
  - Root kits
  - Custom malware (Advanced and persistent)
- Monitoring and tracking capabilities
- Disguised in a separate domain/physical network