Advanced Persistent Threats

George R Magee~ FCNSA, FCNSP, Fortinet
Larry Cushing~ CEO, Unified Technologies

Visit us at Booth #11
An Internet Minute
Spam e-mails intercepted: 50,000
Network intrusion attempts resisted: 41,000
Malware programs neutralized: 10,000
Attempts to access malicious websites blocked: 47,000
Botnet command and control attempts thwarted: 20,000
Website categorization requests: 10 Million

70 Terabytes of Threat Samples
2,500 Application control signatures
70 Intrusion prevention signatures
12,000 Vulnerability management signatures
8,000 Hours of research in labs around the globe
250 Million Rated websites in 78 categories
190,000 New and updated antivirus definitions
900 Web application firewall attack signatures
66 Million New and updated antispam signatures
600,000 URL ratings for web filtering

900 Web application firewall attack signatures
2,500 Application control signatures
70 Intrusion prevention signatures
12,000 Vulnerability management signatures
8,000 Hours of research in labs around the globe
250 Million Rated websites in 78 categories
190,000 New and updated antivirus definitions
900 Web application firewall attack signatures
66 Million New and updated antispam signatures
600,000 URL ratings for web filtering

10 Million Website categorization requests
Agenda

What are APTs?
Malware or Vulnerability?

Case Studies
Latest APT Infiltrations

Defense
Comprehensive, Multi-layer Defenses
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…

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.

- NIST
What are we up against?
Dynamic APT attacks that require proactive protection

ADVANCED
- AV evasion
  - Crypters
- IPS/App evasion
  - Obfuscation
  - Custom protocol
  - Piggybacking
- Sandbox evasion
  - Mouse click
  - Time bomb

PERSISTENT
- Rootkits
  - Hide threats at O/S layer
- Bootkits
  - Invoke at startup
- Process killers

THREATS
- Keyloggers
  - Steal data
- Ransomware
  - Encrypt data and hold for ransom
- HD Wipers

What are Zero-Day attacks?
Previously unseen pieces of code that can only be mitigated, at that time, proactively.
What are APTs?
Defining Advanced Persistent Threats – D.S.I.

**DISGUISE**
- Advanced threats focus on disguise to slip past security detection

**SURVIVABILITY**
- Persistent threats aim to survive on systems as long as possible

**IMPACT**
- Hard drive killers
- Stolen IP, customer data
- Blackmail & Ransom
- Critical infrastructure

Detect Disguise, Kill the Chain
Reduce Survivability, Break Impact
APT Stages - Reconnaissance

- Unlike typical malware infiltration, advanced threats perform initial probes towards targets
- Information gathering such as phishing, social engineering, or social media
APT Stages - Infiltration

- Armed with relevant information, threats infiltrate their targets using various vectors
- Evasion techniques such as crypters, mouse clicks, and piggybacking are used
- Phishing emails, malicious flash (SWF) or PDF documents, malicious websites that attack flaws in browsers like Internet Explorer or Firefox.
- Small scale spear phishing attacks generate little awareness

TARGETS

- Microsoft
- Adobe
- Web browsers
- JAVA
Once the malware is installed, attempts to initiate a call back, using common transmission methods that are allowed by typical security policies. Otherwise, it keeps a low profile, generating no activities that are likely to be noticed. It remains in sleep mode, awaiting further instructions. Increasingly, malware is aware of its environment and won't allow itself to be detected in a virtual machine sandbox.
<table>
<thead>
<tr>
<th>Time/Service</th>
<th>Source</th>
<th>Virus</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNKNO</td>
<td>192.168.60.24</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.24</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.24</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.24</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.24</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.24</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.22</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.22</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.22</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.22</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
<tr>
<td>UNKNO</td>
<td>192.168.60.22</td>
<td>Zeus</td>
<td>host: 91.237.88.230</td>
</tr>
</tbody>
</table>

http://www.fortinet.com/ve?vid=0
Sequence Number: 4241143
Source: 192.168.60.24
Src Port: 56878
Sub Type: infected
Timestamp: 4/24/2014 2:18:00 PM
Virus: Zeus
The exfiltration usually involves the surreptitious delivery of stolen data via often encrypted but common channels, such as HTTPS, back to the command center or to another compromised system controlled by cybercriminals.
APT Stages – Further Exploitation

• With successful communication links between the command center and the compromised hosts, further exploitation is easy to accomplish.
• Malicious acts include attempts to access materials of host connections, such as file shares, cloud-based applications and database credentials.
• Expect lateral moves within the network to expand reach as well as destruction.
Zero-Day Threats

What are they?
Previously unknown code, used with software vulnerabilities

1. MALWARE
   • Very Short Lifespan
     minutes or hours
   • Reformed code
   • Reshaped Crypters / Packers
   • Code is checked against AV detection before an attack is launched

2. VULNERABILITY
   • Long Lifespan
     months or years
   • Security hole that remains unpatched or unknown

EXPLOIT
   • Attack code for a zero-day vulnerability

Can be disclosed or undisclosed

Disclosed zero-days are very dangerous, attack code is widespread
Zero-Day Threats

Why are they significant?
High exploit success rate, no fix available

**IMPACT**
- Exploit can provide full control of vulnerable system
- Targeted or Mass Attack market
- Systems can remain infected for months

**EVASION**
- Transparent end user unaware of attack
- Allows exploit to retain its value
- Profit

**SUCCESSFUL?**
- Very
- Highly prized and hunted
- Sell for Tens of thousands of dollars

**Multiple Revenue Streams**
- Vulnerability knowledge
- Delivery framework creation
- Evasion and repacking and reforming services
Is it just malware?

- Fake certificates
  - Attackers are known to forge SSL certificates to get victims to visit compromised sites.

- Inside jobs (or recruits)
  - In the case of Stuxnet many believe that a sympathetic insider launched attack from a USB drop
Zero-Day : Under the radar

- Potentially most concerning aspect of ATPs is the attack pattern
- When will malware be executed once dropped?
- It’s very possible that today a major power grid is compromised just waiting for the highest bidder.
- Is it a stretch to imagine that every municipal power grid infected by the same malware?
- ...This scenario was reporting by the Wall Street Journal in response to a stimulus package to upgrade the nations power grid systems - http://news.investors.com/040109-472919-not-so-smart-grid.htm

http://www.youtube.com/watch?v=fJyWngDco3g

Electric power supply / Nuclear Generator
Airport, Harbor, subway control systems
Bank, Stocks, Financial systems
Agenda

What are APTs?
Malware or Vulnerability?

Case Studies
Latest APT Infiltrations

Defense
Comprehensive, Multi-layer Defenses
Threat Trends – Mobile (2013)

Recent Android Malware Evolution

- Number of Android samples
- Android samples per day

<table>
<thead>
<tr>
<th>Date</th>
<th>Total number of Android samples</th>
<th>Android samples per day (monthly average)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 01 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feb 01 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar 01 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 01 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May 01 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun 01 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jul 01 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aug 01 2013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Notable Attacks

- Operation Aurora: Google – *botnet agent installed via fake malware prompt*
- Operation Olympic Games – *led to development of Stuxnet, flame, and others*
- RSA Attack – *prime example of spear phishing*
- U.S. Department of Defense – *Breach took place months before actual attack*
- New York Times – *Utilized 45 pieces of custom malware*
- NBC – *Example of drive-by infection using multiple toolkits*
- LinkedIn / Evernote – *May lead to future APT attacks*
Agenda

What are APTs?
Malware or Vulnerability?

Case Studies
Latest APT Infiltrations

Defense
Comprehensive, Multi-layer Defenses
Preparing for the next threat

- Eliminate your blind spots
- Demonstrate your policy compliance
- Lower your response time
- Accelerate adoption of best practices and expert systems
- Reduce the potential of significant or catastrophic loss to reputation or revenue
Protective Measures

• Security Partnerships – ISSA, ISACA, SANS, Vendors
• End user education – Especially those with access to sensitive data
• Network segregation – preventing lateral moves
• Whitelisting – applications, web sites, network resources
• Application Control – Consider identity based application access
• Web Filtering / IP Reputation – Role and geo based filtering
• Data Leak Prevention – protect employees from themselves
• IPS – Consider blended anomaly, signature, and malware solutions
• Proactive patching – Exploit kits contain exploits within hours of patch releases
• Restrict Administrative Roles – Preventing RAT kits
Types of Inspection
Proxy, Stream, and Behavioral

- **Stream AV** – checksum comparison only
- **Proxy AV** – deep inspection, behavior analysis
- **Sandboxing/Behavior Scan** – Full sandbox environment to analyze sample behaviors
Zero-day protection
Comparing Proxy vs. Stream

**Proxy**
- 99.82% Effective

**Stream**
- 98.6% Effective

FortiGuard Internal Test Comparative
Is Sandboxing Useful?
It solves part of the puzzle...

VISIBILITY & REPORTS
• New viral families may not have existing signatures

INCIDENT RESPONSE
• Infection is likely underway, how to deal with it?

NOT USEFUL FOR:
• Mitigation & proactive defense
  • Critical for cases like South Korea attacks, etc
Sandbox Concerns
Evasion Techniques

**Sandbox Evasion Techniques**
- VM detection
- Time bombs
- Debug loops
- Event triggers
  - Mouse clicks
  - System reboots

**Common Sandbox Problems**
- Fixed operating systems
  - Only a few to pick from, and it’s slow
- Fixed software versions
  - Adobe reader, Java
- Attacks very specific to certain versions
- IE: Some require newest version of Java
  - Malware won’t execute in Sandbox
  - Will execute once passed through
APT Strategy: Multi-Layer Defenses

1) Anti-Virus
- Detect known viruses
- Detect new variants (emulation and sandboxing)

2) Web Filtering
- Detect connections going to malware sites
- Typically to download the real malware

3) Botnet / AppCtrl
- Detect connections or traffic going to botnet sites
- Detect known botnet applications

4) IPS
- Block known vulnerabilities
- Including undisclosed vulnerabilities

5) Behavioral
- Sandbox analysis
- Client reputation analysis
Chris Dumais
City of South Portland
Kevin Murphy
Hancock Lumber
Questions for

• George
• Larry
• Chris
• or Kevin?

Visit us at Booth #11!