Spinning the Chess Board

Tom Kellermann, CISM
Chief Cybersecurity Officer, Trend Micro
2014 to 213 BC
Connected Devices Outnumber People
220,000 NEW malware programs EVERY day!

Source: AVTest.Org
Offense Must Inform Defense
Q2 Industry Attack Campaigns

- Government: 81%
- Computer: 4%
- Aerospace: 3%
- Industrial: 3%
- Electrical: 3%
- Telecommunications: 3%
- Military: 3%
- Aviation: 1%
- Financial: 1%
Who Are We Up Against?
Arms Bazaar of Attack Code
## Menu for Full Service Hacking

<table>
<thead>
<tr>
<th>Service</th>
<th>Monthly</th>
<th>Onetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Service</td>
<td>$25</td>
<td>$0</td>
</tr>
<tr>
<td>Botnet Framework</td>
<td>$40</td>
<td>$125</td>
</tr>
<tr>
<td>Bulletproof hosting</td>
<td>$52</td>
<td>$0</td>
</tr>
<tr>
<td>Exploit Kit</td>
<td>$38</td>
<td>$120</td>
</tr>
<tr>
<td>Domain names</td>
<td>$0</td>
<td>$20</td>
</tr>
<tr>
<td>Dropper file and crypt</td>
<td>$70</td>
<td>$25</td>
</tr>
<tr>
<td>Modules</td>
<td>$8</td>
<td>$80</td>
</tr>
</tbody>
</table>

**Total:** $225 $370
Exploit Kits: Do-it-Yourself

Reference: Jones 2012 [2]
Thriving Underground Market

- Malware offered for $249 with a service level agreement (SLA) and replacement warranty if the creation is detected by any antivirus within 9 months.
Banking Crime Kits Decrease in Price

Underground Price Changes for Basic Online Banking Toolkits

These are estimated going rates. Note that ZeuS and SpyEye have been around since before 2010.
GameOverZeus: GOZ
Zberb
A Comparison of Russian and Chinese Hackers
Weapons Grade Arsenal

• Greater reconnaissance
• Utilization of 0-days
• Undetectable by anti-virus
• Able to withstand normal disinfection methods like reinstalling OS
• Calling home is undetected by DLPs and IPS/IDS
• Data extraction, command and control even across an air gap
What are the Trends of Attack?
Q2 Serious Java Vuls

- **HIGH**: 14
- **MEDIUM**: 8
- **LOW**: 3

- **Patched**
- **Unpatched**

Date: 8/19/2014
Offense Must Inform Defense
Exfiltration: Most Used APPs and Protocols
Evasions

- Packers
- Compressors
- Metamorphism
- Port Binding
- Polymorphism
- Virtual Machine
- Sandbox
Dropping In
What are the new attack vectors?
Watering Hole Attacks

Source: Trend Micro Q2’14 Treat Roundup Report
Malicious URLs by Country

- United States: 25%
- Netherlands: 3%
- Germany: 3%
- China: 3%
- Russia: 3%
- France: 3%
- United Kingdom: 2%
- South Korea: 1%
- Japan: 1%
- Czech Republic: 1%
- Others: 55%

8/19/2014
Island Hopping
81% Have Not Updated SLAs
Man-in-the-Browser Attacks
The Evolution of Mobile Attacks
Mobile Ransomware: Svpeng & Locker
Proximity Attacks Realized
Geopolitics as Harbingers for Attack
Energetic Bear
2014 Cyber Attack Trends

1. Island Hopping
2. Mobile Malware/Proximity attacks
3. Cross-Platform Attacks
4. Man-in-the-Browser Attacks
5. Watering Hole Attacks
6. Ransomware
7. *Cloud Attacks*
Foiling the Digital Insider
Opportunities to Detect the Breach

- Failed/Irregular Logins
- Security Warnings
- Check for Injected DNS Records
- Abnormal Protocols
- Increased Email Activity
- Strange Large Files
- Abnormal Connections
Advanced Persistent Response
Advanced Malware Detection

Attacker Activity Detection

Contextual Threat Analysis

Threat Impact Assessment
Risk Management in 2014

1. Conduct Pen test of all third parties.
2. Use Two-factor authentication.
3. Conduct egress filtering.
4. Deploy file integrity monitoring.
5. Implement virtual shielding for zero day exploits.
6. Deploy both an MDM and Mobile Application Reputation software.
7. Deploy a DLP.
8. Implement whitelisting.
9. Manage the crypto keys for your cloud data.
10. Implement DMARC.
11. Deploy context aware Threat Intelligence.
Breach Detection with Deep Discovery

360 Degree Detection
- Custom sandboxing
  - Matching precise customer specs
  - Mobile, Mac, and more
- Beyond malware
  - C&C comms, attacker activity
- Beyond web & email traffic
  - 80+ protocols/apps over all ports

Custom Intelligence
- Smart Protection Network & Threat Researchers
- Threat Connect for custom intel
Threat Connect Portal – Impact Analysis

**Threat profile:** What are the characteristics, origins and variants of this malware.

**Related IPs/Domains:** What are the known C&C comms for this attack.

**Attack Group/Campaign:** Who and what is behind this threat.

**Containment and remediation:** What to look for, how to eradicate.

Accessed directly from Deep Discovery Console
Situational Awareness
Securing your journey to the cloud