Observations on Emerging Threats

Paul Ferguson
Threat Research
Trend Micro, Inc.
Cupertino, California  USA
“Trend Micro's Threat Research group is specially tasked with looking forward on the threat landscape and working with technology and/or various product development groups inside the company to ensure that, as a company, we deliver the appropriate security solutions to address emerging threats to our customers. To accomplish this requires our threat research group to understand, explore, and deconstruct various malicious technologies, campaigns, vulnerabilities, and exploits which are currently being perpetrated on victims today.”
Introduction

- Evolution, Commoditization, Professionalism of Exploit Kits
- Increasing Sophistication of Traffic Direction Systems (TDS)
- Smaller, Diversified Botnets
- Modularization
- Evolution of Mobile Threats
- Continued Exploitation of Social Networks
- Critical Infrastructure Attacks
- HTML5 “Exploitation”
- More Data Breaches via Targeted Attacks (APT)
- “Hard-to-Reach” Relocation of Criminal Activity
Evolution, Commoditization, Professionalism of Exploit Kits

- Virtually **ALL** “Professional” Eastern European criminals are using various Exploit Kits to increase the possibility of successful compromise.
- Generally used only by Eastern European criminals.
- Example Evolution: Crimepack → Phoenix → Eleonore → Blackhole
- Each step of evolution is an incremental improvement on previous iteration.
- Blackhole Exploit Kit is currently the most popular kit.
- Uses heuristics to determine what vulnerabilities may exist on the end-system to determine what payload to deliver.
Increasing Sophistication of Traffic Direction Systems (TDS)

- TDS are used to redirect a victim to specific landing page based on some criteria (below).
- Redirection criteria is generally referrer (affiliate ID).
- Primary used to direct traffic by pay-per-install or pay-per-click campaign in order to manage monetization scheme(s).
- Manage/Tracks Statistics, e.g. Hits, By Country, Referrers, etc.
- Currently Most Popular: Sutra TDS
- TDS are generally used to redirect victim to an Exploit Kit, Fake AV, etc., depending on affiliate campaign.
### Traffic Statistics

**2010/06/13**

Top 'Raw hits' = 6662

<table>
<thead>
<tr>
<th>Referers</th>
<th>Raw hits</th>
<th>Unique hits</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://xxlib.org/">http://xxlib.org/</a></td>
<td>6253</td>
<td>2837</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=5422">http://protizer.net/new_stat.php?id=5422</a></td>
<td>4576</td>
<td>2875</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=1944">http://protizer.net/new_stat.php?id=1944</a></td>
<td>4081</td>
<td>2965</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=10115">http://protizer.net/new_stat.php?id=10115</a></td>
<td>1922</td>
<td>1488</td>
</tr>
<tr>
<td><a href="http://micro-win.com/">http://micro-win.com/</a></td>
<td>1290</td>
<td>347</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=1166">http://protizer.net/new_stat.php?id=1166</a></td>
<td>844</td>
<td>602</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=23633">http://protizer.net/new_stat.php?id=23633</a></td>
<td>801</td>
<td>184</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=17490">http://protizer.net/new_stat.php?id=17490</a></td>
<td>712</td>
<td>372</td>
</tr>
<tr>
<td><a href="http://hitlife.net/sex_online_game/">http://hitlife.net/sex_online_game/</a></td>
<td>677</td>
<td>422</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=7544">http://protizer.net/new_stat.php?id=7544</a></td>
<td>659</td>
<td>188</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=286">http://protizer.net/new_stat.php?id=286</a></td>
<td>508</td>
<td>385</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=18872">http://protizer.net/new_stat.php?id=18872</a></td>
<td>443</td>
<td>272</td>
</tr>
<tr>
<td><a href="http://protizer.net/new_stat.php?id=2732">http://protizer.net/new_stat.php?id=2732</a></td>
<td>437</td>
<td>231</td>
</tr>
<tr>
<td><a href="http://micro-win.com/index.php">http://micro-win.com/index.php</a></td>
<td>390</td>
<td>68</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hour</th>
<th>Raw hits</th>
<th>Uniques</th>
<th>Proxies</th>
<th>Without referer</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>57629</td>
<td>23617 (41.0%)</td>
<td>9599 (16.7%)</td>
<td>801 (1.4%)</td>
</tr>
<tr>
<td>00</td>
<td>6662</td>
<td>2684 (40.3%)</td>
<td>1141 (17.1%)</td>
<td>110 (1.7%)</td>
</tr>
<tr>
<td>01</td>
<td>5939</td>
<td>2229 (37.5%)</td>
<td>1005 (16.9%)</td>
<td>154 (2.6%)</td>
</tr>
<tr>
<td>02</td>
<td>4342</td>
<td>1535 (35.4%)</td>
<td>721 (16.6%)</td>
<td>95 (2.2%)</td>
</tr>
<tr>
<td>03</td>
<td>3188</td>
<td>1030 (32.3%)</td>
<td>664 (20.8%)</td>
<td>81 (2.5%)</td>
</tr>
<tr>
<td>04</td>
<td>2290</td>
<td>732 (32.0%)</td>
<td>462 (20.2%)</td>
<td>96 (4.2%)</td>
</tr>
<tr>
<td>05</td>
<td>1756</td>
<td>637 (36.4%)</td>
<td>288 (16.4%)</td>
<td>8 (0.5%)</td>
</tr>
</tbody>
</table>

**Countries**

- **PL** Poland: 125 (0) 27
- **CH** Switzerland: 115 (0) 4
- **FR** France: 109 (0) 16
- **NO** Norway: 106 (0) 21
- **IE** Ireland: 97 (0) 5
Smaller, More Diversified Botnets

- Decline of Large, Monolithic Botnets (e.g. Storm, Conficker, Waledac, etc.)
- Diversification as a result of take-downs impact
- Bot infrastructure is “cheap” but seeding takes time
- Most of the time & effort is in the seeding, e.g. Initial spam runs or drive-by (or exploit kit) campaigns, etc.
- Banking Trojan Botnets are a great example: Customization by Each “Owner/Operator”, hundreds of individual “botnets” may exists in parallel.
Emergence of Modularization

• Banking Trojans Modularization: Screen Grabber, Back-Connects, Web Injects, etc.
• Exploit Kit Modularization: Modules added for new exploits (per-CVE/Exploit, per-browser, per-plugin, etc.)
• We expect to see further evolution of the modularization concept in new “plug 'n play” Trojan and exploit kits, as well as other platforms.
Evolution of Mobile Threats

- Most Mobile Threats thus far can be considered “Proof-of-Concept”
- Majority have been legitimate Apps which have been Trojanized
- Majority have been re-packaged Trojan Apps that appear in “illegitimate” App markets.
- “Professional Criminals” will ramp up targeting of Mobile platforms with wider adoption of e-Commerce Applications, Near-Field Communications (NFC), etc. where money can be stolen or redirected.
Social Network: The Low-Hanging Fruit

- Social Networking platforms allow criminals unique opportunities to get close to their victims.
- Users generally publish too much personal information on Social Network platforms which can be used against them in a criminal campaign.
- Humans are generally naive, too trusting, easily baited, tricked, fooled, or just plain thoughtless and reckless in their online behavior.
- No obvious reason to think that this will change.
Critical Infrastructure: Some Hard Lessons Will be Learned

- Just like other private networks, many (most?) connected to the Internet in some way.
- Just like other privately owned infrastructure, a lot of utilities/industrial control systems are not well-secured or have poor security posture.
- Transportation, Manufacturing, Electricity, Water Processing, etc.
- We expect to see an escalation of security incidents involving “critical infrastructure”, and perhaps some serious reconsideration of how these systems are connected to the rest of the world.
New Exploitation Vectors with HTML5

- With HTML5, attackers can now create a botnet which will run on any OS, in any location, on any device.
- HTML5 is heavily memory-based, barely touches the disk, and may be difficult to detect via traditional antivirus.
- More enabling of XSS, Click-jacking, Tab-Napping, CSRF/CSOF
- Web Sockets allows surreptitious delivery mechanism for malicious content (exists today with Flash).
- Similar in fashion to JAVA, more ubiquitous adoption of HTML5 will help foster a more homogenous attack surface.
More Data Breaches via APTs

- Data Breaches via “Targeted Attacks” or “APTs” share many similar foundations in human behavior, trust, and susceptibility to being “socially-engineered” – these will continue to proliferate due to the ease in which they can be executed by determined attackers.

- Observation: Virtually ALL of the successful targeted attacks we have observed have used very simple social-engineering tricks.

- Once attackers have successfully gained a presence, they use various modified programs to move laterally, find targeted resources, and exfiltrate data.
Criminals Move To More 'Resistant' Services

- Professional criminals (especially) have refined the art of “maximizing their windows of opportunity”.
- They learn which services allow them the maximum amount of maneuverability and long-lived operations (protection to operate).
- Observation: Criminals already know which hosting providers, domain registrar/reseller, upstream connectivity, etc., provides them the most “window of opportunity”.
- As some emerging economies become more connected to the Internet, there is generally a lag between connectivity/services and security “policing”. We predict the Africa continent, as it becomes better connected to the rest of world, will be a haven for criminal hosting.
Summary

• “Snapshot in time.”
• “…wait 15 minutes and it will change.” Weather colloquialism.
• The biggest challenge for any organization is to adapt quickly to a changing threat landscape. Be nimble.
• Threats manifest themselves in the most bizarre, and sometimes mundane, ways.