The Exploit Intelligence Project

Dan Guido
dguido@isecpartners.com
07/25/2011
Intro and Agenda

• Talk series discussing intelligence-driven security
  • Provide actual data on attacker characteristics
  • Provide analysis tradecraft to analyze it
    • Intrusion kill chains
    • Attacker characterization
    • Adversarial attack graphs

• Informed defense is more effective and less costly
  • Less hypothetical, more verifiable
  • Defenses supported by observation
  • “Technology doesn’t beat determination”
Let’s Talk About Vulnerabilities

*IBM X-Force 2010 Trend and Risk Report*
How many vulnerabilities did you have to pay attention to avoid SpyEye, Zeus, Gozi, Clampi, etc?

2010: 13

2009: 14
What are we doing wrong?
Maslow’s Internet Threat Hierarchy

# of Attacks

- APT
- Targeted
- Mass Malware

Value of Data Loss

- IP
- $$$
- Banking Credentials
Mass Malware

How does it work?
Gain Exposure

Malicious Ads

SEO

Compromised Friends

SQL Injection
Weaponize Capabilities

5-20 exploits, $200-$2000 dollars
Establish Delivery Network
Exploit Targets
Install Malware
Establish Command and Control
Leads to Cyber Pompeii
The Intrusion Kill Chain

- Systematic process that an intrusion must follow
  - Deficiency in one step will disrupt the process

- Evolves response beyond point of compromise
  - Prevents myopic focus on vulnerabilities or malware
  - Identifies attacker reuse of tools and infrastructure

- Guides our analysis and implementation of defenses
  - Align defenses to specific processes an attacker takes
  - Force attackers to make difficult strategic adjustments
Spy vs Spy

Millions of Infected Sites → Expose → Blacklists, Categorization

Thousands of Vulnerabilities → Weaponize → IDS, Patches, Secure Code

Thousands of IPs → Deliver → Blacklists

Tens of Applications → Exploit → ???

Millions of Malware Samples → Install → AV

Thousands of IPs → C2 → Blacklists, IDS, DLP

??? → Actions → ???
Going on the Offensive

FERRARI TANK
Send your enemies stampeding over each other in fear.

In style.
Exploit Kit Popularity (Q1 2011)

*ThreatGRID Data
Collected Data Sources

• Blackhole
• Bleeding Life
• CrimePack
  • 3.1.3, 3.0, 2.2.8, 2.2.1
• Eleonore
  • 1.6, 1.4.4, 1.4.1, 1.3.2
• Fragus
• JustExploit
• Liberty
  • 2.1.0, 1.0.7

• LuckySploit
• Phoenix
  • 2.5, 2.4, 2.3, 2.2, 2.1, 2.0
• SEO Sploit pack
• Siberia
• Unique Pack
• WebAttacker
• YES
• Zombie
Mapping of Kits to Exploits + Metadata

Phoenix Exploit Kit

- CVE-2009-0836
- CVE-2009-0927
- CVE-2009-1869
- CVE-2010-0188
- CVE-2010-0840
- CVE-2010-0842
- CVE-2010-1297
- CVE-2010-1818
- CVE-2010-1885
- CVE-2010-2883

Affected Vendor: Apple
Affected Product: Quicktime
Type: Memory Corruption
Bypasses: DEP, ASLR

Discovered: 08/30/2010
By: Ruben Santamarta
MSF: 08/30/2010
MSF Rank: Great

ExploitDB-14843
OSVDB-67705
Zero Day Initiative? No
Discovery Location? Whitehat
Exploitation is focused on dominant platforms (check statowl.com)
Vulnerability Origin (2009-2010)

Where were massively exploited vulnerabilities first disclosed?

- **Targeted Attack**
- **Zero-day Disclosure**
- **ZDI**
- **Vendor Advisory (Non-ZDI)**
- **Unknown Vulnerability**

![Graph showing vulnerability origin](image)

- 2010
- 2009
Effective Analysis

YEP, IT'S WOOD
Evaluate Your Defenses

- Intelligence gives us data to evaluate our defenses and verify they work as intended

- Jan 1, 2009 – what can we put in place to mitigate all exploits for the next two years?
  - Restrictions: *no patching allowed*
  - There are ALWAYS more bugs

- Corporate Desktop circa 2009
  - Internet Explorer 7, Firefox 3.0
  - Adobe Reader 9, Java, Quicktime, Flash, Office 2007
  - Windows XP SP3
# Effective Defenses (2009-2010)

## Memory Corruption (19)

<table>
<thead>
<tr>
<th>Defeated by</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DEP</td>
<td>14</td>
</tr>
<tr>
<td>ASLR</td>
<td>17</td>
</tr>
<tr>
<td>EMET</td>
<td>19</td>
</tr>
</tbody>
</table>

## Logic Flaws (8)

<table>
<thead>
<tr>
<th>Flaw</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No Java in Internet Zone</td>
<td>4</td>
</tr>
<tr>
<td>No EXEs in PDFs</td>
<td>1</td>
</tr>
<tr>
<td>No Firefox or FoxIt Reader</td>
<td>2</td>
</tr>
</tbody>
</table>
“I don’t presume that a bug discovered by a researcher can’t be exploited by malware writers. Some are very capable.”
DEP Bypasses (2009-2010)

<table>
<thead>
<tr>
<th>Reader</th>
<th>CoolType SING</th>
<th>APT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader</td>
<td>libTIFF</td>
<td>APT</td>
</tr>
<tr>
<td>Flash</td>
<td>newfunction</td>
<td>APT</td>
</tr>
<tr>
<td>Java</td>
<td>getSoundBank</td>
<td>kf</td>
</tr>
<tr>
<td>Quicktime</td>
<td>_Marshaled_pUnk</td>
<td>reversemode</td>
</tr>
</tbody>
</table>

Even the “advanced” exploits come with heavy limitations
## Logic Flaws

<table>
<thead>
<tr>
<th>Technology</th>
<th>Vulnerability</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>Calendar Deserialization</td>
<td>Sami</td>
</tr>
<tr>
<td>Java</td>
<td>Trusted Method Chaining</td>
<td>Sami</td>
</tr>
<tr>
<td>Java</td>
<td>WebStart</td>
<td>Tavis</td>
</tr>
<tr>
<td>Java</td>
<td>URI Argument Injection</td>
<td>Tavis</td>
</tr>
<tr>
<td>IE</td>
<td>Help Center XSS</td>
<td>Tavis</td>
</tr>
<tr>
<td>FoxIt</td>
<td>Auth Bypass</td>
<td>Didier</td>
</tr>
<tr>
<td>Reader</td>
<td>PDF Social Engineering</td>
<td>Colin</td>
</tr>
<tr>
<td>Firefox</td>
<td>SessionStore</td>
<td>moz_bug_r_a4</td>
</tr>
</tbody>
</table>
# The Myth of Sophistication

<table>
<thead>
<tr>
<th>DEP Bypasses (5)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Developed by APT</td>
<td>3</td>
</tr>
<tr>
<td>Developed by Whitehats</td>
<td>2</td>
</tr>
<tr>
<td>Developed by Malware Authors</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logic Flaws (8)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovered by APT</td>
<td>0</td>
</tr>
<tr>
<td>Discovered by Whitehats</td>
<td>8 (!)</td>
</tr>
<tr>
<td>Discovered by Malware Authors</td>
<td>0</td>
</tr>
</tbody>
</table>
Public Exploit Code Preferred

Targeted Attack  Zero-day Disclosure  ZDI  Vendor Advisory (Non-ZDI)  Unknown Vulnerability

Gradient of Information Detail

2010  2009

iSEC PARTNERS
The Defender’s Dilemma?

Defending successfully is making no mistakes.

Don’t make mistakes and you won’t get hacked, guaranteed.
Basic Browser Attack Graph

1. Expose
2. Weaponize
3. Deliver
4. Exploit
5. Install
6. C2
7. Actions

---

Malicious HTML

- Google Chrome
- IE8
- IE7, Plugins, Java, Flash

---

DEP/ASLR Bypass

- Sandbox Escape
- Integrity Escalation
Attack Graph Traversals (2009-2010)

Google Chrome → DEP/ASLR Bypass → Sandbox Escape

IE8 → DEP/ASLR Bypass → Integrity Escalation

IE7, Plugins, Java, Flash, etc on XP
Intelligence-Driven Conclusions

• Start making vaccines and fighting your adversaries
  • Find their resource constraints and attack them!
  • Benchmark your defenses against attack data
  • Create and maintain an attacker’s dilemma

• Mass Malware Authors Case Study
  • Can’t write exploits and rely on public disclosures
  • Can’t evade simple defensive techniques
  • Choose predictably easy targets
Related Work

• UCSD, Oakland 2011 – Holistic Analysis of Spam
  • “Click Trajectories: End-to-End Analysis of the Spam Value Chain”

• Mike Cloppert, ICIW 2011 – Holistic Analysis of APT
  • “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”

• Dino Dai Zovi, SOURCE Boston 2011 – Attack Graphs
  • “Attacker Math 101”

• Microsoft, SRD Blog – Exploit Mitigations
  • “Mitigating Software Vulnerabilities” Whitepaper