Trends in Malware

DRAFT OUTLINE
Security is often a game of cat and mouse as security professionals and attackers each vie to stay one step ahead of the other. In this race for dominance, attackers are developing ever more sophisticated malware exploits. Modern malware increasingly preys on human naivety, burrows deep within operating systems, and is even able to change its own software code to evade detection. In this session we will examine the current malware landscape, looking at who is behind the attacks, how it works, and, most importantly, what we can do to counter the threat.
## Recent, High Profile Attacks

<table>
<thead>
<tr>
<th>Target</th>
<th>Facility</th>
<th>Adversary</th>
<th>Means</th>
<th>Attack Goal</th>
<th>Result</th>
<th>Strategic Goal</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telvent Canada Ltd</td>
<td>Electricity</td>
<td>Chinese hackers</td>
<td>Malware</td>
<td>Steal intellectual property</td>
<td>Penetrated security defenses and obtained software and blueprints related to SCADA system</td>
<td>Unknown</td>
<td>Undetermined</td>
</tr>
<tr>
<td>Aramco, Saudi Arabia</td>
<td>Oil</td>
<td>Hacktivist</td>
<td>Malware (Shamoon)</td>
<td>Information destruction, steal intellectual property</td>
<td>Erased hard drives</td>
<td>Stated: End government oppression, particularly in middle east</td>
<td>First publicly known case of hacktivist group using state developed malware</td>
</tr>
<tr>
<td>RSA</td>
<td>IT</td>
<td>Chinese hackers</td>
<td>Malware (Excel Spreadsheet)</td>
<td>Steal intellectual property</td>
<td>Compromised RSA SecureID token generation</td>
<td>Speculation: Steal US jet fighter blueprints from LM</td>
<td>Speculation: Acceleration of Chinese military capability</td>
</tr>
<tr>
<td>Natanz Nuclear Facility, Iran</td>
<td>Nuclear</td>
<td>US &amp; Israeli Government</td>
<td>Malware (Stuxnet)</td>
<td>Halt or delay uranium enrichment</td>
<td>Destroyed centrifuges</td>
<td>Delay Iran from obtaining nuclear material</td>
<td>First publicly known, attributed use of cyber weapon by national government</td>
</tr>
</tbody>
</table>
Malware Track Record

• 2010: On average, only 53% of malware detected on download*

• 2011: 250% Increase in unique malware domains**

• 2011: 49% of breaches used malware***

• 2012: On average, 2 new, unique pieces of malware per day****

* 2010 NSS Labs study (www.nsslabs.com)
** 2011 Cisco Global Threat report (www.cisco.com)
*** 2011 Verizon Data Breach Investigations Report
**** 2012 ZDNET http://www.zdnet.com/blog/bott/the-malware-numbers-game-how-many-viruses-are-out-there/4783
What is Malware

Malware, short for malicious software, is software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer system.

- Wikipedia
Characteristics

• Proliferate (spread)
• Infect (infiltrate)
• Conceal (hide)
• Compromise (disrupt, exfiltrate)
Malware Types

- Virus (self replicates by attaching to another program or file)
- Worms (replicates independent of another program)
- Trojan Horses (masquerades as legitimate file or program)
- Rootkits (gain privileged access to a machine while concealing itself)
- Spyware (collect information from target system)
- Adware (delivers advertisements with or without consent)
Actors

- Government & Military
- Organized Crime
- Terrorists
- Activists
- Opportunists (just for kicks, profit, show-off skills)
Early Malware

- 1988 - Morris Worm (remotely connect to a UNIX process, overwrite memory (buffer overflow) and gain access to the machine)

- 2001 - NIMDA (spread through email or webs. Would modify or replace legitimate files on system and open remote access with admin privileges.)

- 2005 - Sony BMG rootkit (Installed by inserting SONY music CD into PC. Designed to prevent copying of CD - XCP. Software hid itself and opened vulnerabilities that subsequent malware exploited)
Traditional Defense

- Manual Inspection & Removal (use tools to look for files or settings and remove or restore)
- Anti-Virus (look for file or settings signature and remove or restore)
- Intrusion Detection / Protection (look for packet types, formats, patterns and block or redirect)
- Firewall (filter, permit or deny traffic)
- Sandboxing (limit behavior - restrict application rights/access, lock-down systems, segment networks, etc.)
Modern Malware

• Customized & Targeted
• Polymorphic (pieces of code in the malware change for each distribution - e.g. shifting encryption, data insertion, changing code run order)
• Remotely controlled with encrypted communications (botnets - provide agility and flexibility)
• Persistent and intelligent (probe network to find more vulnerabilities, adjust tactics, blend in, low and slow)
• Beyond computers (mobile, industrial)
Integrated Attacks

1. Infiltrate: spam, phishing, P2P networks, web browsing, social media, social engineering,

2. Infect: trojan horse, virus, worm

3. Persist & Spread: worm, botnet, rootkit

4. Attack: Steal, SPAM, DDoS
Modern Defense

• Architecture (policy, governance, operations, capabilities)

• Intelligence-led threat defense, not just vulnerability elimination

• Contextual & anomaly-based threat detection

• Automated, policy-based enforcement
Security Architecture

• Security starts with goals (i.e. what’s important to the business)
• Requires policy and governance that aligns with goals
• Leverages cyber defense operations that implement policy and governance
• Builds on an infrastructure platform that provides trust, visibility & resilience
Intelligence-led Threat Defense

• Assess target, adversary, risk, means as a basis for developing defenses

• Balance across prevention, preparation, response, and recovery

• Build sources of local and global intelligence
Context & Anomaly-based Threat detection

• Complexity of modern malware means static, signature-based systems alone do not work

• Monitor a broad scope of behaviors to fingerprint attacks

• Correlate with risk of compromise
Automated, Policy-Based Enforcement

- User, device, location, and resources are no longer fixed
- Identity is the new perimeter
- Infrastructure must leverage policy to dynamically enforce access as user, device, location, and resources shift