You are the weakest link!
The human factor in security

David Emm
Global Research and Analysis Team
The growing malware threat
From one every MINUTE to one every SECOND

- Malware from downloads
- Malware in KL databases January 2013
- New threats every day
The growing malware threat
From one every MINUTE to one every SECOND

<table>
<thead>
<tr>
<th>LATEST VIRUSES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 June 2012</strong></td>
</tr>
<tr>
<td>Trojan-PSW.Win32.Bjlog.deqj</td>
</tr>
<tr>
<td>not-a-virus:RiskTool.Win32.Hooker.mj</td>
</tr>
<tr>
<td>Trojan-PSW.Win32.Bjlog.deqo</td>
</tr>
<tr>
<td>Trojan-Dropper.Win32.Dapato.bfrr</td>
</tr>
<tr>
<td>Trojan-PSW.Win32.Bjlog.deqi</td>
</tr>
<tr>
<td>Trojan.Win32.Jorik.Vobfus.eoxw</td>
</tr>
<tr>
<td>Trojan.Win32.Genome.afmuj</td>
</tr>
<tr>
<td>Backdoor.Win32.LolBot.baha</td>
</tr>
<tr>
<td>Trojan-FakeAV.Win32.SmartFixer.no</td>
</tr>
<tr>
<td>Backdoor.Win32.Shiz.etcq</td>
</tr>
</tbody>
</table>
The fast-growing MOBILE malware threat
Sophisticated threats: code obfuscation
Sophisticated threats: rootkits and bootkits
Sophisticated threats: fake or stolen digital certificates

- **Common Name:** JMicron Technology Corp.
- **Status:** Revoked
- **Validity (GMT):** Jun 18, 2009 - Jul 25, 2012
- **Class:** Digital ID Class 3 - Software
- **Organization:** JMicron Technology Corp.
- **Organization Unit:** Digital ID Class 3 - Microsoft System Design
- **State:** Taiwan
- **City/Location:** Hsinchu
- **Country:** TW
- **Serial Number:** 476f49f4c959f656e9aa1ebc
- **Issuer Digest:** 4e302ea92e9d99951ec2bf

**Digital Signature Details:**
- **Signer Information:**
  - **Name:** MS
  - **E-mail:** Not available
  - **Signing Time:** Tuesday, December 28, 2010 4:54:40 PM

**Certificate Information:**
- **Issued By:** Microsoft LSRA PA
- **Valid From:** 2/20/2010 to 2/20/2012

**Certificate Details:**
- **Confirm this is the correct certificate before performing any further actions.**
- **Digital Signature Information:** A certificate was explicitly revoked by its issuer.
Types of attack

Cyber-weapons:
- ‘Destroyers’
- Espionage programs
- Cyber-sabotage tools

Targeted attacks

‘Traditional’ cybercrime
‘Hacking’ humans
What is to be done?
‘Patching’ humans

- It’s a human problem
  - It needs a HR solution
  - Not IT
- Education - not training
  - Security is a mindset
  - Not [just] following rules
  - It’s like housework!
- Psychology is important
  - It’s about people - not ‘users’
- The medium is the message
  - Imaginative ways to reach out to employees
  - Social engineering works!
  - Self-interest
Business security

Comprehensive protection

- Signatures
- Heuristics
- HIPS
- Application control
- Device control
- Web control
- Whitelisting
- Encryption
- Cloud-based and endpoint

Security strategy

- Risk assessment
- Establish policies and procedures
- Create outbreak response plan
- Deploy appropriate solutions
- Define and update patch policy
- Develop staff education
- Document the strategy
Thank you