The Latest Malware Threats Against Your PC

Tom Chen
SMU, Dept of Electrical Engineering
Dallas, Texas 75275
tchen@engr.smu.edu
www.engr.smu.edu/~tchen
Malware (Malicious Software)

Internet

Your PC

Worms
Spyware
Viruses
Bots
Backdoors
Trojans
Malware Damages

- $169-204 billion: total damages from malware in 2004 $[mi2g$
- $300$ malware cost per Windows PC, on average $[mi2g$
- Malware was highest security loss to organizations in 2004 $[FBI/SANS survey$:
  - $67,000$ damages per organization
  - $75\%$ organizations hit by malware attack
Protection?

Malware can be downloaded unknowingly

Via email

New attacks can evade detection

10 new software vulnerabilities discovered daily
Spyware

- Spyware: programs that secretly monitor user activities (visited Websites, confidential data, passwords) and reports this data through network

- Often installed secretly:
  - Bundled with freeware
  - Obscure EULA (end user license agreement)
  - Downloaded by malicious Web sites
Spyware (cont)

• Estimated 55-88% PCs are infected by spyware
  - 42% users had no idea how spyware was installed [Ponemon Institute survey]
  - Average PC has 25 spyware infections [WebRoot]

• 89,806 Web pages found with infectious spyware in first half 2005 [WebRoot]
### Top Spyware 2004*

<table>
<thead>
<tr>
<th>Spyware</th>
<th>Behavior</th>
<th>Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purity Scan</td>
<td>Displays pop-ups when user is online</td>
<td>Tricks user by claiming to delete porn</td>
</tr>
<tr>
<td>n-CASE</td>
<td>Displays pop-up ads</td>
<td>Bundled with freeware</td>
</tr>
<tr>
<td>Claria</td>
<td>Displays banner ads based on surfing habits</td>
<td>Bundled with freeware</td>
</tr>
<tr>
<td>CoolWebSearch</td>
<td>Hijacks Web searches and IE settings</td>
<td>Install using malicious HTML applications or security flaws</td>
</tr>
</tbody>
</table>

*WebRoot*
Worms

- Worms are automated self-replicating programs
  - Probe for new targets with vulnerabilities through network
  - Copy themselves to targets

Propagation mechanism | Payload
Worm Propagation

- Most prevalent worms spread by emailing themselves (Netsky, Sober, Mytob)
- Some also spread by peer-to-peer file sharing and instant messaging
- Multiple variants of Cabir, first worm for Symbian smart phones, now seen ‘in the wild’
  - Also seen Commwarrior, first smart phone worm to spread by MMS (multimedia messaging service)
Common Worm Payloads

- Disables antivirus and personal firewalls by killing antivirus processes and deleting critical registry files
- Downloads new code updates from the Internet
- Installs other malware (bots, Trojans, backdoors, keystroke loggers, rootkits)
Trojan Horses

- Trojan horse: programs with hidden malicious functions, or hidden programs
  - Backdoors: allow secret remote access (Sub7, Netbus, Back Orifice)
  - Keystroke loggers: secretly record all user’s keystrokes (Bugbear, Lirva worms)
  - Bots: listen for remote commands (spam, denial of service attack) in a ‘bot net’ (Randex, Spybot, Gaobot)
  - Rootkits: totally ‘own’ victims
Bots

- 6,361 new variants of Spybot; 1,412 new variants of Randex; 1,121 new variants of Gaobot seen in first half 2005 [Symantec]

- Estimated 1-2 million PCs infected with bots [Honeynet Project]
  - Largest bot net seen is 50,000 bots
  - 10,866 bots seen active on average day [Symantec]
  - 1/3 bots in UK where broadband is commonplace
Rootkits

- Malware of choice: kernel rootkits (Knark, Adore)

- Attackers with ‘root/admin’ access can hack the operating system kernel

- Target PC is totally ‘owned’ by remote attacker
  - Kernel rootkits can be impossible to detect

- Probably an increasing threat in future
Conclusions

• Just a sample of the wild Internet -- it pays to be overly protective
  - Keep antivirus software current and use restrictive firewalls
  - Malware is hard to detect and always evolving

• Our research in automated worm quarantine and use of ordinary traffic controls