Addressing Spyware and other potentially unwanted software

Meng-Chow Kang, CISSP, CISA
Chief Security & Privacy Advisor, Asia Pacific Region
Microsoft Corporation

The 32nd APECTEL Working Group Meeting, Seoul, Korea
September 5-9, 2005

A Snapshot of the Problem

- **Prevalence**
  - 50% of users sampled by Customer Services & Support (CSS) have Spyware on their machines (2004)
  - Watson crash reports (Jan. – April 2004)
    - Responsible for 45% - 60% of Watson error reports in the top 100 WinXP buckets

- **Support cost**
  - CSS: Spyware was their #1 issue
    - Directly linked to 1% and likely linked to >19% of CSS calls
  - Top support issue for OEMs
    - Likely linked to ~30% of calls for top 3 OEMs
    - Dell: #1 support issue
    - HP: #2 support call generator
    - A large MS customer: #2 issue in internal helpdesk calls (behind password-related issue)

- **Impacts**
  - Reliability
  - Privacy
  - Annoyance
  - Security
  - Performance
### Modus Operandi

- Bundled with freeware
- Spyware “required” by Web sites
- Hide installation program behind “interesting information” link
- Drive-by downloads (vulnerability exploitation)
- Fake “Cancel” button as part of an image
- Auto-update feature (EULA)

Deception, Social Engineering, Exploitation

### “Deceptive Software”

**What is it?**

Software that installs & runs without adequate consent
- “Spyware” and unauthorized “adware”
- Programs that “hijack” the default home page or search engine
- Dialers, cycle stealers, and keystroke loggers

**Why can’t we just detect and stop these behaviors?**

With adequate consent many features can be desirable
- Custom advertising through personalization
- Reduced cost of software in exchange for advertising
- Cycle sharing for public benefit
A New Kind of Problem

- “Bad” software with a “good” business model
  - Many users are willing to trade privacy information for free software & information
  - Many companies are willing to spend money buying spyware-collected information
  - Many bundled spyware programs were clearly stated in the freeware EULA
  - Some spyware programs do provide a Remove option in Add/Remove Programs
  - “Anti-spyware” very different from “anti-virus”

Classifying Spyware

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection</td>
<td>No potential harm</td>
<td>Notepad</td>
</tr>
<tr>
<td>Advertising</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Changes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Resource Use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Activity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Spyware and other Potentially Unwanted Software:
Programs that perform certain functions without appropriate user consent and control

- Clearly malicious (virus, worm, trojan)
- Sasser
Addressing Spyware Challenges

*Empower users to make informed decisions to control what software installs and runs on their computer*

- **Technology**: Help protect users from spyware and other potentially unwanted software. Update system and application to stay current against exploitation.
- **Guidance & Engagement**: Provide a trusted resource for how to remove and avoid spyware and other unwanted software.
- **Industry Collaboration**: Collaborate with industry players to identify and address spyware and other unwanted software.
- **Legislation & Enforcement**: Discourage deceptive software development.

---

What Enterprises Can Do Today

- **Policy and Procedures**
  - Implement Acceptable Use policy for corporate IT resources
  - Set restrictive browser settings
  - Implement Software Restriction Policies
  - Create response procedures for spyware infections
- **User Awareness**
  - Safe web browsing
  - Dangers of installing unknown software
  - Recognizing symptoms of an infected machine
- **Technology**
  - Stay current with security updates
  - Secure the Browser: Implement XP SP2 enhancements to IE
  - Utilize desktop FW, up-to-date AV, and Network FW
  - Evaluate user controlled or centrally managed anti-spyware solutions based on needs
Spectrum of Deception

<table>
<thead>
<tr>
<th>Deceptive</th>
<th>Exemplary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violates Law</td>
<td>Follows Min Practices</td>
</tr>
<tr>
<td>Confusing Experience</td>
<td>Follows Best Practices</td>
</tr>
<tr>
<td>Enforcement</td>
<td></td>
</tr>
<tr>
<td>Prevention/Detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Best Practice/Cert Programs</td>
</tr>
</tbody>
</table>

Best Practice Takeaways

*How To Stay Out Of Trouble*

- Prominent notice and opt-in for:
  - Sharing personal info
  - Programs that display stand-alone ads
  - Programs without complete uninstall or disable
- Prominent notice and opt-in or opt-out for:
  - Changes to browser home or search page
- Easy control of stand-alone ad programs
  - Ability to stop future ads
  - Visibility into source of ads