Technical & Educational Strategies for combating Spyware

BSI
Federal Office for Information Security
Germany

Thomas Veit
* Definition Spyware

* Current situation & trends

=> Comprehensive approach:

**Culture of Security**

<table>
<thead>
<tr>
<th>Government / Organizations</th>
<th>Citizens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendors</td>
<td>Providers</td>
</tr>
</tbody>
</table>
1st: What do we call Spyware?

(very) general suggestion for a definition:

Spyware is:

Any program that does send local information to some remote system without the users consent

Bots / Trojans / Viruses might be included by this definition in principle

"Adware" would not be included in this definition, since the user is presumed to give consent before or while installing respective software

System Management Software would not be included as well, since a general consent by the user is presumed as given
recent BSI Status report:
Information Security in Germany / 2004

Percentage of infected Emails, discovered at central gateways of Federal Government Network (IVBB)
... Evolution of Malicious software

- hybrid, multifunctional malicious code
- highly distributed & coordinated, incl. encryption
- "for buy" on the Net, criminal intent
- with little, or without coordination
- single function
- simple viruses, trojans

~ 1990  2005

sophistication

one particular aspect: MIV  →
Multiple Infection Vectors

Variety of vectors for compromise of systems

* Automated execution of malicious WebScripts
* Execution of malicious Email-Attachments
* Direct intrusion via open port / vulnerability
* download malicious software & execution,
  & combinations
Evolution of targets

- specific & unspecific selection of systems to compromise

unspecific targets

Specifically targeted
- against certain sector,
- against certain organization,
- against certain systems

cases observed in recent past
=> Comprehensive approach necessary ...
... single/isolated technical measures are not enough

lots of "easy targets"

significant quantity of compromised systems

convergence of malicious features

variety of vectors to compromise systems

seemingly significant amount of criminal intent & money involved

significant quality of distributed malicious architecture
... by all responsible actors

<table>
<thead>
<tr>
<th>Government / Organizations</th>
<th>Citizens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendors</td>
<td>Providers</td>
</tr>
</tbody>
</table>
Vendors / Suppliers

Security of products, suggested actions:

(preventive)
- built-in security by design
  * not just single features, but structural
  * caveat: complexity

(reactive)
- implement vulnerability management procedures
- recognize cooperation with CERTs

- pre-configure products with appropriate balance between security and functionality (examples)
Government / Organizations

- Implement Comprehensive Security Framework

  * policy / guidelines / architecture / international cooperation

  * education of users on how to work securely on the Net
    e.g. awareness campaign

  * include security requirements for the procurement of software

  * apply technical measures
    - central security management of clients
    - in principle, multiple security checks
      * e.g. central + client AntiVirus / Firewall

  * implement vulnerability management procedures
Citizens

- get informed about security issues
  (e.g. <www.bsi-fuer-buerger.de> in Germany)

* behave accordingly (Email, Scripting, Download)

* use technical measures
  - AntiVirus, Personal Firewall
Providers

- provide a
  "secure Internet access package"
  for those customers who want it

  * including "basic port filtering"
  * provide recommendation for up2date
    AntiVirus & Personal Firewall
If all players act together:

=> a significant reduction of spyware & malicious program dissemination would be possible