

Protecting Your Network: Mitigating Spyware in Organizations

Organizations can employ the following techniques to reduce the IT costs, abuse of system resources, and productivity loss associated with malicious and commercial spyware.

Educate Employees and Other Network Users

- Require network users to agree to an Acceptable Use Policy indicating unauthorized programs can be blocked at the gateway and removed from PCs.
- Teach employees and other computer users to understand that many "free" programs and services on the Internet install spyware that drastically slows PCs, installs annoying pop ups, and steals private and corporate information. (See ASC's "Protecting Your Computer: Avoiding and Removing Spyware" document for additional end-user training advice.)
- Train Help Desk staff to recognize the less overt spyware symptoms (very long boot up, slow and erratic application performance, crashing), so accurate root-cause can be assessed and proper remediation taken.

Block Spyware at the Gateway

Gateway proxies or firewalls can be configured to prevent spyware from reaching networked PCs via combinations of the following:

- Define policy to prevent "drive by" downloads (non-approved CAB and OCX files).
- Define policy to prevent executable downloads from known spyware sites (identified by content filtering lists).
- Define policy to prevent executable downloads from suspected/high-risk sites (sites in categories with high incidents of spyware).
- Scan files at the gateway for known spyware code.
- Define policy to block PC communication to known spyware "phone home" sites and report which PCs are likely infected with spyware.
- Analyze logs of PC communications for unduly high-traffic/high-frequency destinations.
- Maintain strong anti-spam protection to limit spyware hidden inside spam.

Protect Corporate PCs from Spyware

Desktop anti-spyware applications can detect and remove spyware trying to execute on PCs, and perform best when you:

- Maintain up-to-date detection patterns and software updates.
- Select desktop security software that can be centrally deployed and managed.
- Deploy technology from different anti-spyware researchers at the desktop and gateway to provide "defense-in-depth."
- Maintain current operating system and browser patches to minimize vulnerability to security exploits.
- Ensure web browsers are set to a minimum security and privacy threshold of "medium."
- Do not allow users to surf Internet while logged in with "Administrator" privileges.
- Maintain a list of allowable software and/or executable files and run a weekly scheduled check against PCs in the network. Check results for non-standard entries.
- Consider re-imaging chronically spyware-infected PCs.

This content can be freely copied and used as long as you make no substantive changes and clearly give ASC credit. For details, see <http://www.cdt.org/about/copyright.php>.