



Spyware: Situation Summary

**Wes Ames, Associate Technical Fellow
Boeing IT Computing Security Infrastructure
March 2005**

February 2006
Privacy and Security Conference
Victoria, BC, Canada

Malicious Software Review

- Viruses
- Worms
- Trojans
- Spyware
- Adware
- Browser Hijackers
- Rootkits

Currently increasing Risks

- Bot-Nets
- Root-kits
- Mobile Computing Attacks
- Phishing
- Man In The Middle Attacks
- Spyware
- Traces and footprints

Spyware – How does it work?

- **Types of Spyware**
- **What is Spyware?**
- **Similar to computer virus evolution**
- **Levels of Influence**
- **Methods of Incursion**
- **What to do**

Types of Spyware

- Investigational Spyware
 - ✓ Individually targeted objectives
 - ✓ Some legitimate, some not
 - ✓ Same tools used by legitimate and illegitimate
- Advertising Industry Spyware
 - ✓ Indiscriminate targets
 - ✓ Some legitimate, some not
 - ✓ Rarely desirable

What is Spyware?

- Spyware is software that runs surreptitiously on a system, tracking user behavior or data and reporting to a remote host.
- It may be passive, simply identifying a discrete user to a group of affiliated web sites, or...
- It may be active, holding control of your machine and working on a private agenda, unbeknownst to the system operator.
- In all cases, it will attempt to remain undetected, to avoid removal.

Similar to Computer Virus Evolution

- Started as nuisance factor
- General skepticism regarding threat
- Disagreement on degree of threat
- Rapid growth of threat
- Inadequate legal tools
- No tools from traditional vendors
- Shareware tools not suited to enterprise-wide use

Levels of Influence

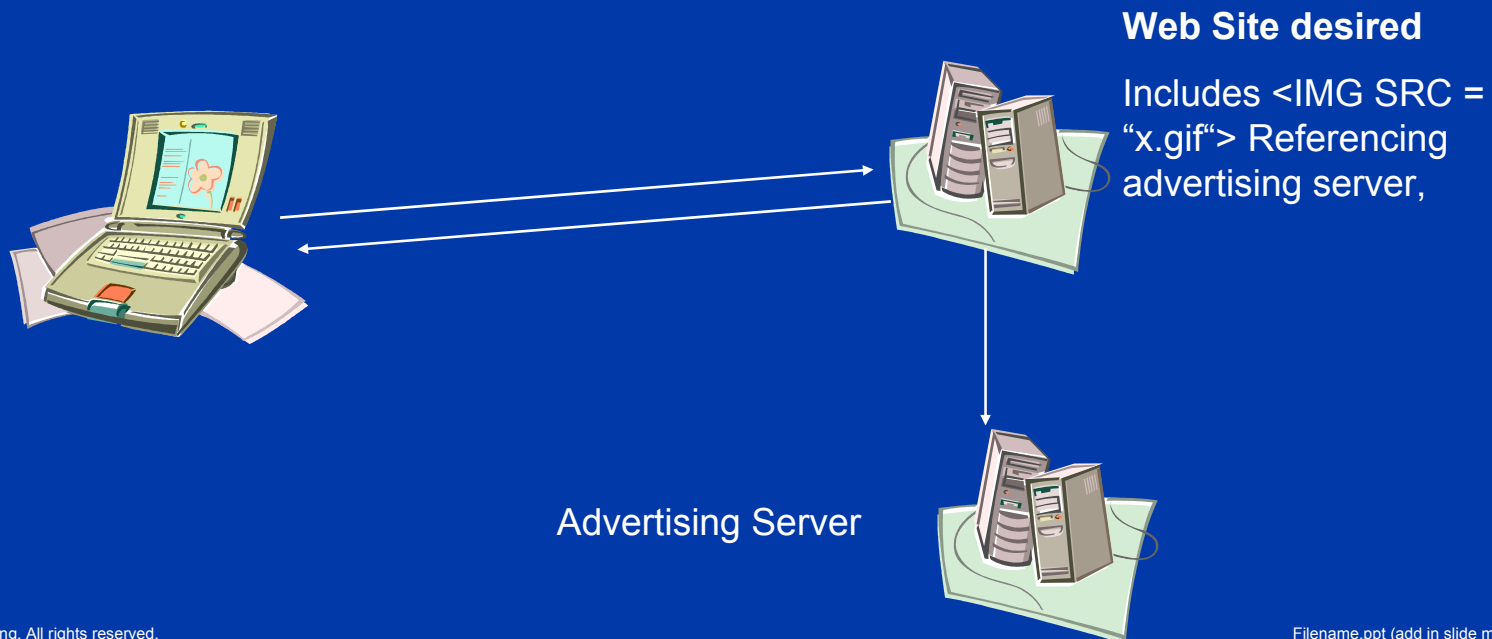
- Cookies – Single Site – Not Spyware
 - ✓ Allow a single site to ID user
 - ✓ Used to recall user history and preferences

Levels of Influence, continued

- Cookies – Single Site – Not Spyware
 - ✓ Cookies allow a single site to ID user
 - ✓ Used to recall user history and preferences
- Cookies – GUID – Low level Spyware
 - ✓ Affiliation of sites, tracks user activity
 - ✓ Creates shared database of user data

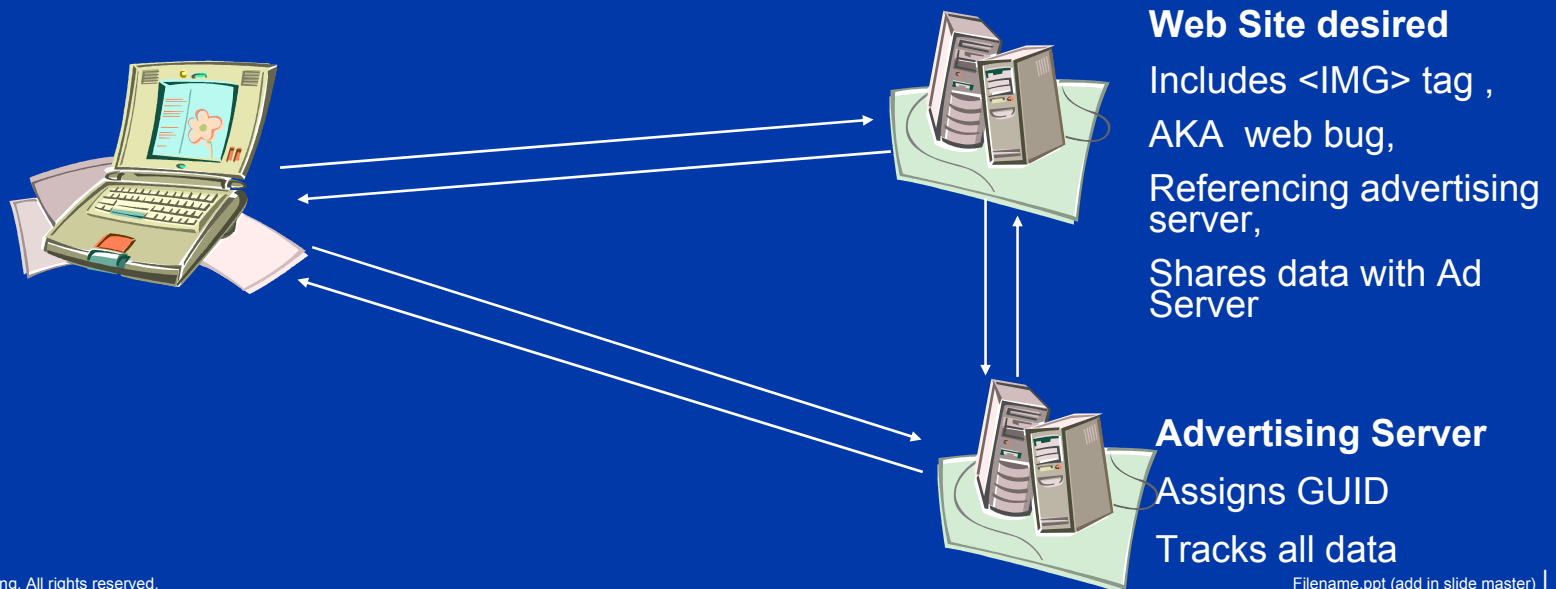
Levels of Influence, continued

- Cookies – GUID – Low level Spyware
 - ✓ Affiliation of sites, tracks user activity
 - ✓ Creates shared database of user data



Levels of Influence, continued

- Cookies – GUID – Low level Spyware
 - Affiliation of sites, tracks user activity
 - Creates shared database of user data



Levels of Influence, continued

- Cookies – Single Site – Not Spyware
 - ✓ Cookies allow a single site to ID user
 - ✓ Used to recall user history and preferences
- Cookies – GUID – Low level Spyware
 - ✓ Affiliation of sites, tracks user activity
 - ✓ Creates shared database of user data
- DLL/COM/EXE – Executable, Malignant Spyware
 - ✓ Once installed, no limits on operations
 - Updates, new installations, open to Internet, capture keystrokes, transmit data, etc.
 - May include Rootkit techniques

Methods of Incursion

- Web travel acquires cookies with GUID
 - ✓ Single site cookies OK
 - ✓ Affiliated cookies result in data collection
- Software download
 - ✓ May Include undesired spyware applications
 - Added to download package
 - Host application Trojan (Hotbar, Gator)
- Hidden install (Active-X, Java)

Risks

- Data Miners

- ✓ Database of information on each user
- ✓ Data is shared across sites
- ✓ Data is sold

- Executable Spyware

- ✓ Gains control of PC
- ✓ Not limited to any actions
- ✓ May install updates or other software
- ✓ Frequently leave back door vulnerabilities
- ✓ Carefully hides itself
- ✓ Many additions/modifications to systems

Symptoms

- Instability
 - Long waits
 - Crashes
 - Hangs
- Death by Pop-ups !
- Spam – Spam – Spam !

Security Vendors are Stepping Up

- Anti-Virus
 - ✓ Adding spyware detection and removal
 - ✓ Some blocking capabilities
 - ✓ Not yet full-featured
 - ✓ Some additional cost modules
- Firewall
 - ✓ Primarily blocking capabilities
 - ✓ Some exclusion capabilities (application recognition)
- IPS
 - ✓ Adding spyware recognition and blocking
 - ✓ Both Software and Appliance devices are adding features

New Vendors are Stepping In

- Anti-Spyware Vendors
 - ✓ Began by doing only spyware
 - ✓ Offered leading capabilities (Block, detect, remove)
 - ✓ Now Adding more features
 - ✓ Firewall
 - ✓ Anti-Virus
 - ✓ Common GUI Security Interface

Game Changers

What are the developments that could dramatically impact Anti-Spyware strategy?

- Legislation
- User Awareness
- Coordination of Layered Security Enhancements
 - ✓ Perimeter, Firewall, AV, IPS, more?
- Microsoft influence on field
- New Players (both teams)

