Spyware – Linkages to Malware and its Affects
A Multi-Layered Approach to Stopping Information Theft

Kim Duffy
Internet Security Systems

Agenda

• What are the trends?
• Why should I be concerned?
• How does Spyware work?
• How can it be addressed?
• A Case Study
Headlines

It's a really hostile environment!

88% of home PC’s and
87% of Corporate PC’s

.....Have at least one piece of Spyware On-board!

ISS Company Background

- Founded in 1994
- 1998 IPO – NASDAQ: ISSX
- 1,200 employees in 20 countries
- Pioneer and world leader in intrusion prevention

- Pioneer and world leader in vulnerability assessment
- Created standard of cybersecurity research with X-Force research team
What are the Trends?

- One in every 3 companies have detected spyware on the network
- 80% of all “connected” PC’s have spyware
- More than 7,000 spyware programs are known to exist
- IDC survey says 4th greatest risk to enterprise network security
- SPYBLOCK Part II...
Why should I be concerned?

• Spyware can undermine good security
  – Search and send confidential information
  – Delete or modify registry settings
  – Key logging
  – Disable software applications (e.g. security)
  – Install back doors
  – Take over peripherals

Web Cam... or Spy Cam?

Trojans - 101

• The Trojan Horse
  – Gains unauthorised access without your knowledge
  – Appears to be benign
  – Attacker gains access
  – Executes code
Spyware - 101

• Like Trojans, appears to be legitimate software
• Performs malicious activity without your knowledge

Adware - 101

• Originally not malicious intent
• Considered less harmful
• Displays Pop-Ups
• Highly profitable for the hacker
• Catalyst for the development of anti-Spyware
• Often bundled with “freeware” or “shareware”
Why should I be concerned?

• Spyware has a financial/resource cost
  – Computer resources…memory, processor
  – Network resources… data transmission
  – Employee productivity… spam, removal

How Does Spyware Work?

• Spyware generally propagates via web sites, email messages and pop-ups
• Images-based infection is an emerging threat
  – Ipods
• Techniques
  – Personalization Cookies
  – Tracking Cookies
  – Trojans
  – Drive-by Downloads
  – Hacking
  – Parasitic or Piggybacking Apps
How Does Spyware Work?

• Trojans > Spyware > Adware

• What to watch for…
  – Long boot times
  – Slow browsing, unexpected network activity
  – Error messages “Insufficient Memory”
  – Increased frequency of Pop-up ads

Prevention ALWAYS Beats Reaction

Periodic “search & destroy” is reactive
  • Too late for many
  • Relies on diligence of user
  • Typical of free spyware utilities

Automatic “blocking” is preventive
  • Prevents spyware from compromising systems and confidential data
  • Requires advanced R&D
Spyware Prevention: Multilayered Technologies

1. URL Filtering
   – Prevent user access to known distributors of spyware applications

2. Intrusion Prevention (IPS)
   – Prevent ActiveX installers & “Phone Home” communications

3. Virus Prevention (VPS)
   – Prevent browser hijackers & key loggers

4. Application & Communication Control
   – Prevent “rogue” application installation and “Phone Home” communications

Spyware Prevention: Multilayered Architecture

Gateway Protection
– Prevent spyware from entering the network

Network Protection
– Prevent spyware from propagating and communicating

Host Protection
– Prevent spyware from damaging hosts
....What to do now?

Awareness
Education
Preparedness

Security is a Journey…not a Destination!

Questions?