

Security Strategy to address Spyware threats

Dixon Ho
 Chief Security Officer
 Microsoft Hong Kong Limited
 Email: dixonho@microsoft.com

What is the objective of implementing Security?

Our objective is to build an environment as secure as a **Castle**



Industry Survey Data

National Cyber Security Alliance Survey in 2004

Consumer

- 91% of broadband consumers affected by "spyware"/"adware"
- Avg of 5+ "spyware"/"adware" programs per machine

Corporate

- Web@work survey of IT managers:
 - 92% believe their firms are infected with "spyware"
 - Estimate 29% of corporate machines (on avg) are infected

Spyware Incident Report

- From March 04 to Dec 04 (World-wide) - The number of Spyware Incident increase from 500,000 to 1,700,000

(by CA Spyware Research)

Spyware will cost you time and money

- Microsoft estimates that spyware is responsible for 50% of all PC crashes
- Dell reports 20% of its technical support calls involve Spyware

(Sources: Information Week, April 26, 2004)

What Is Spyware?

- Although there is no formal definition, Spyware is generally considered to be any software with unauthorized access to your system and relays your private information to a third party without proper authorization.

What Spyware will do?

- Monitor and relay your Web browsing behavior
- Email logging
- Instant messaging usage and snapshots
- Modifying application/OS behavior
- Carrier of the virus
- Keystroke tracking and capture

Risks and Impacts:

- Annoyance of your normal operation
- Reduce PC performance
- Increase bandwidth usage
- **The source of virus out-break**
- **Theft of confidential data**

Signs of Spyware

- I see pop-up advertisements all the time
- My settings have changed and I can't change them back to the way they were
- My Web browser contains additional components that I don't remember downloading
- My computer seems sluggish

How do people get infected?

- Web browsing
- Unauthorized download
- File swapping
- Unauthorized Email attachments by spam mail
- Instant messaging
- Installing "legitimate software"

Variety and Risk Level

- Adware and cookies (Risk level 25%) – reduce performance and non-critical information collection
 - Track user activity on the internet
 - Collect personal information
- Pop-up Ads (Risk level 40%) – impact performance heavily, freeze machine and non-critical information collection
 - Collect information for cookies
 - Interrupt user transaction on internet
 - Flood users with Ads and freeze machines
 - Install utilities that modify user services

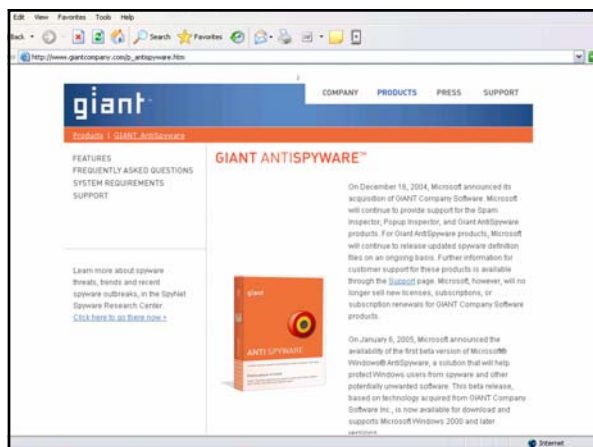
Variety and Risk Level

- Hijackers (Risk level 70%) – impact performance heavily, freeze machine and critical information security issues
 - Modify content of web pages
 - Block access to websites
 - Redirect users to unintended websites
 - Install hidden/backdoor processes and services that are tightly bound to OS
 - Disrupt websites used for mission critical applications
- Spyware <Overt> (Risk level 95%) – critical information security issues that may not easily be discovered
 - Gains a remote control capability, which includes searching and reading local files
 - Has a self-updating capability
 - Often includes a network sniffer
 - Can usually activate webcam or microphone
 - Usually logs all keystrokes

How to address the Spyware Issue

- **Use Anti-Spyware Solution**
 - Too bad, today it only can cater 60 – 70% of the problem
- **User Education**
 - Do not Open Email attachment without verification with the sender
 - Do not browse any non-trustable site
 - Do not download any freeware or shareware from a site that is not trustable
 - Do not do any e-banking or personal information related activity at the public PC (e.g. Airport, Starbuck, or MTR Central Station)
 - **“Remember you always have a chance to pay a price if you do not pay enough attention in Spyware threats”**

Microsoft AntiSpyware Beta 1



MS AntiSpyware

- **Reject known spyware**
 - The Internet's most comprehensive library of spyware signatures ensures that your computer always knows exactly what to eliminate.
- **Stops spyware in its tracks**
 - More than 50 real-time security agents monitor and prevent potential spyware threats before they can damage your system.
- **Benefit from SpyNet™: the Internet's first neighborhood spyware watch**
 - As soon as one of the 100,000 SpyNet™ members detects a new spyware string, we update our library of spyware.

MS AntiSpyware

- **Enables customers to:**
 - Detect and remove spyware—
 - Known spyware can be quickly and easily removed from a PC.
 - Improve Internet browsing safety—
 - Continuous protection guards over 50 ways websites and programs can put spyware on a PC.
 - Stop the latest threats—
 - Signatures for new spyware identified by the SpyNet™ community and Microsoft researchers can be automatically downloaded to a PC, helping to stop new threats quickly.

Beta1 Summary

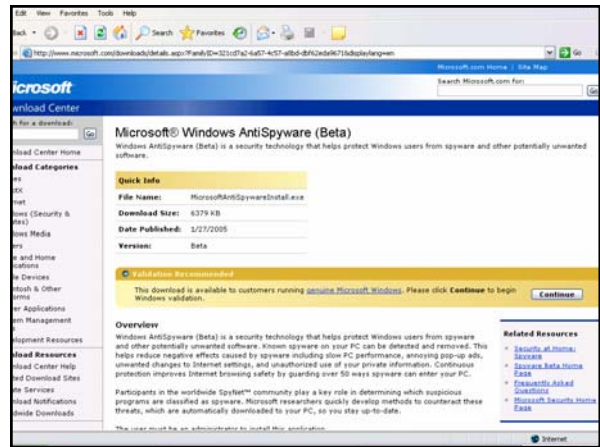
- **Public Beta release 1/6**
 - Just 21 days after our acquisition of GIANT Company Software, Inc.
- **Feature enhancements in Beta1:**
 - Microsoft re-branding
 - Security improvements
 - Privacy improvements
 - Temporarily removed spyware cookie feature
 - Permanently removed System Inoculation & File Shredder

Platforms

- Supported Platforms
 - Windows 2000 Professional (all SPs)
 - Windows XP Professional/Home Edition (all SPs)
 - SP2 install
 - Windows 2003 Server
 - AMD 64
- We will probably deprecate
 - Windows 98/98SE/Me
- Locals
 - Run on locals
 - Need local Administrative rights (in current Beta)

Download the beta of Microsoft Anti-Spyware software

- <http://www.microsoft.com/spyware>



AntiSpyware Demo & Walkthrough

This block contains a collage of screenshots from the Microsoft AntiSpyware (Beta) software. The top-left screenshot shows the 'Microsoft Windows AntiSpyware (Beta) Setup' window with 'Next' and 'Cancel' buttons. The top-right screenshot shows the 'Microsoft Windows AntiSpyware (Beta) Spyware Scan' window with a 'Run Scan Now' button. The bottom-left screenshot shows the 'Microsoft Windows AntiSpyware (Beta) Spyware Scan' window displaying scan results, including '11 spyware threats detected'. The bottom-right screenshot shows the 'Microsoft Windows AntiSpyware (Beta) Spyware Scan' window displaying scan results, including '11 spyware threats detected'.

This screenshot shows the 'Microsoft AntiSpyware (Beta) Spyware Scan' window. The 'Run Scan Now' button is highlighted. The 'Last Scan Run' section shows the scan date and time, along with a list of scan results: 47 memory locations scanned, 1 infected; 20204 files checked, 20 infected; 9883 registry locations checked, 173 infected; 1 cookie scanned, 0 infected. The 'Quick Status' section shows: Total spyware scans run: 1, Total spyware detected: 11, Spyware in quarantine: 0. The 'Schedule Scan Details' section shows: Runs at 2:00 AM every day, Click to schedule.

