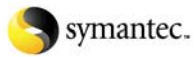




RESPONDING TO SPYWARE

CHUA KAY CHUAN
*Government Relations Representative for
Asia Pacific & Japan*
5 September 2005, Seoul



Agenda

- Threat Landscape Evolution
- Cost & Impact of Spyware/Adware
- Responding to Spyware



About Symantec

- ▶ World leader in information security, availability, and integrity
- ▶ Operate in more than 40 countries, employing 14,000 people in research, development and delivery of solutions
- ▶ Publish the *Internet Security Threat Report*, the authoritative analysis of the evolving threat landscape
- ▶ Key player in industry movements, including the Anti-Spyware Coalition



Evolving Threat Landscape

- ▶ Yesterday
 - Fame was the objective
 - Mass, undirected attacks
- ▶ Today & Tomorrow
 - Fortune is now the objective
 - with criminals using technology to perform targeted attacks
 - New risk/attack vectors
 - Amplified use of technology and computer speed giving rise to fast spread



Prevalence of Spyware/Adware

- ▶ October 2004 AOL/NCSA Online Safety Study
 - 80 percent of scanned computers actually had spyware or adware

- ▶ Earthlink Report
 - Scan of 3 million computers systems over nine months found 83 million instances of spyware.



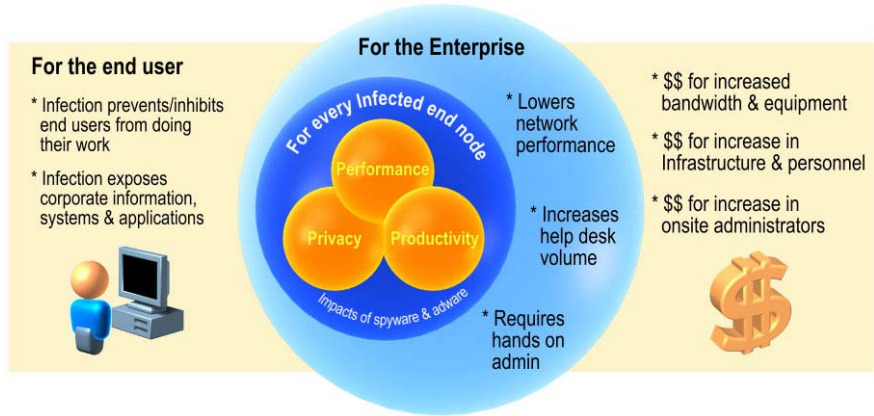
The Prevalence of Adware/Spyware

- ▶ A February 2005 study by Symantec using an unprotected PC connected to Internet

- ▶ 1 hour of browsing popular websites resulted in:
 - 359 adware risks after browsing popular child-focused websites
 - 17 adware and 2 spyware risks from 6 sports-related websites
 - 23 adware and 4 spyware risks from 6 gaming-related websites
 - 64 adware and 2 spyware risks from 5 travel-related websites



The Cost of Spyware and Adware



As prevalence increases so will costs



Consumer Impact of Adware/Spyware

Los Angeles Times, 1/14/2005

A computer owner for seven years, Kasul did a little shopping online. Her husband used the machine to help manage some rental property, and her 16-year-old daughter wrote term papers for school.

Then her daughter went on the Internet to research a paper on the issue of breast-feeding in public. As if she had typed in a magic word, spyware ads for porn sites popped up and wouldn't go away. Soon the computer was unusable. It took more than three weeks and \$300 to get the thing working again, by which time all the family's data had been wiped out. Now Kasul sends her daughter to use the computers at school or the library.

"I don't do much shopping online anymore because that scares me," Kasul said. "I go to the store."



"No More Internet for Them"



Consumer Impact of Adware/Spyware

Big Brother has your number (and your name)

Cnet Download.com, 2005

My first experience with spyware was the most horrible. It happened about two years ago, when the concept of spyware and adware was still new.

I was browsing dating Web sites, when only a few seconds later I received an e-mail titled "Looking for a Date Samer?" At first, I thought it was just a strange coincidence, but later **it started to freak me out, especially when I began to get weird e-mails containing my personal information** that were geared toward my taste in products.

Even more bizarre was that my computer would start my dial-up connection in the middle of the night. I'd wake up to see myself connected to the Web. Finally, I downloaded Ad-Aware, and all those problems became history.

Source: "Spyware Horror Stories" Cnet Download.com, 2005
<http://www.download.com/1200-2023-5137405.html>



Spyware Creating a Crisis of Confidence

- ▶ **NCSA-AOL Survey (Oct '04)**
 - Do you believe your computer has spyware on it?
 - 53% "yes," 47% "no"
 - 80% actually had spyware on their computer
- ▶ **CSIA Voters Survey (June '05)**
 - 93% of likely voters believe spyware is a serious problem and 61% believe Congress should be doing more to battle identify theft online
 - 48% are *avoiding* making purchases on line because of fear over identify theft
- ▶ **Pew Study(July 05):**
 - 90% of Internet users have changed online behavior out of fear of spyware



Responding to Spyware/Adware



A New Comprehensive Approach Needed

- ▶ Standardization & Classification of Risks
- ▶ Legislation and policy responses
- ▶ Research & Development



Symantec's Spyware Definition

Programs that have the ability to scan systems or **monitor activity and relay information to other computers or locations in cyber-space**. Among the information that may be actively or passively gathered and disseminated by Spyware: passwords, log-in details, account numbers, **personal information**, individual files or other personal documents. Spyware may also gather and distribute information related to the user's computer, applications running on the computer, Internet browser usage or other computing habits.



Symantec's Adware Definition

Programs that facilitate delivery of advertising content to the user through their own window, or by utilizing another program's interface. In some cases, these programs may gather information from the user's computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer or other location in cyber-space.



Develop a Risk Impact Model

Shift from viruses to spyware requires different approach

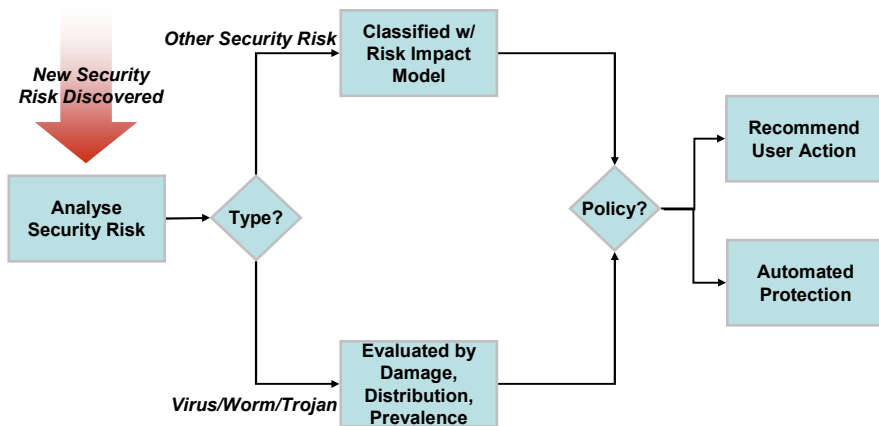
- ▶ Changes in the risk landscape require a new approach. Deterministic approaches to virus, removal and blanket policies to remove all spyware programs do not suffice
- ▶ Grey areas of legitimacy emphasise need for flexibility and the need to allow individuals to determine actions based on preferences
- ▶ Symantec Security Response's **Risk Impact Model** evaluates computer applications to help users determine whether or not removal is desirable.



Benefits of the Risk Impact Model

- ▶ No value judgment made on adware business models
- ▶ Adware and Spyware are not categorized as 'Malicious Code' but evaluation is based on the objectivity of potential security risks
- ▶ Users are empowered to make informed decisions
- ▶ Allows flexibility for users to exercise their preferences, while security industry provides the tools
- ▶ All organizations can be treated fairly and consistently

New Protection Process *Including risk impact analysis*



Legislative & Policy Response

- ▶ Good Samaritan
- ▶ Security Exemption
- ▶ Enhancement of EULAs
- ▶ Strengthening the penalties for cyber security crime



Why is Good Samaritan Language Needed?

The Mercury News
MercuryNews.com

Posted on Wed, Jun. 22, 2005

Don't handcuff spyware fighters

SECURITY FIRMS SHOULDN'T BE HELD LIABLE FOR GETTING RID OF PESTS

Mercury News Editorial

The best defense against computer pests such as adware and spyware is a good offense. Today, PC users can go on the offensive with one of dozens of anti-spyware programs that are available online or on store shelves. These programs detect, flag and remove -- or advise the user to remove -- the intrusive programs that, according to surveys, plague an estimated 90 percent of all PCs on the Internet.

Some makers of spyware and adware are challenging the anti-spyware makers in a game of chicken. They're claiming that detecting or removing their programs amounts to interference with their business. Some have threatened anti-spyware makers with litigation.



Why is Good Samaritan Language Needed?

- ▶ Consumers should have the right to know what are on their machines
- ▶ Governments need to clarify the role and posture of security companies
- ▶ Prevent frivolous lawsuits, ultimately translating into higher costs and prices in general.



Spyware Legal Pressure

- ▶ Threat of Libel Suits
- ▶ Threat of Tort Claims
- ▶ Sneaky Programming and Attorney's as part of a bigger strategy



Security Exemption

- Behavior vs Technology mandates
 - Legislation should be technology neutral
- Provides a protection for security company technology



The Limitations of EULAs

- ▶ Many spyware and adware companies currently use EULAs as a way of leading consumers into a false sense of security that their rights are protected.
- ▶ User license agreements can be used to:
 - Attempt to limit user's rights to remove software
 - Attempt to pressure anti-spyware vendors to reduce coverage
 - Attempt to minimize legal risk to allegations of fraud
 - Assuage their corporate advertisers that they are legitimate
 - Assist in public and investor relations work



Specific Language in some EULAs

- ▶ “To improve the features or functions of the xxxxxx AdServer and/or xxxxxx and/or third-party xxxxxx-Supported Software, ***we may occasionally install and/or update software components,*** “
- ▶ “These are collectively referred to herein as “Enhancement Technologies”. ***For example, these Enhancement Technologies may be used to deliver audio and visual effects such as animation, video and sound, or to provide enhanced services such as secure coupon printing.***”
- ▶ “Please note that removing all xxxxxx-Supported Software ***does not necessarily cause the removal of any Enhancement Technologies (as described above).***”



Enhancing EULAs

- ▶ Users should be given clear notice and choice regarding the installation of monitoring software on their systems
- ▶ Users should be able to remove or uninstall said software easily and completely without damage to the computer or the information stored on it



Conclusion

- ▶ Prevalence of spyware is increasing, and should be seen in the context of the evolving threat landscape
- ▶ The costs of spyware and adware to consumers and organisations will also correspondingly increase
- ▶ Requires a new, comprehensive approach by industry and governments to address this issue.



Thank You

Chua Kay Chuan
*Government Relations Representative
for Asia-Pacific & Japan*
E-Mail: kaychuan_chua@symantec.com

