



Public commentary for the FTC Spyware Workshop

First - How do you define spyware for purposes of designing your Ad-Aware product and how does that product work?

We no longer use the term "Spyware" as it has become misused and misunderstood. Strictly speaking we define it based on the semantics. The first part is the word "Spy" which implies that someone or something is secretly collecting information. This also implies that the activity is overtly designed to be hidden, without notice, stealthy, deceptive, etc. The second part refers to the agent; in this case it denotes that this is a software application or "ware". As we view this in the most conservative way possible it is extremely limited and does nothing to assist the user with understanding the underlying privacy/security risk. We recognized this early in the development of Ad-aware so created what we feel is a more appropriate method for determining what should and will be detected by our software.

Our method is based on behavior and perceived intent of the developer rather than relying on "fashionable" definitions. Please see the following page on our web site where we have detailed this:

<http://www.lavasoft.de/support/resources/>

Ad-aware is designed to detect, report, and then give the user the option to remove said content at their discretion. We do not suggest or recommend that the content be removed rather we feel strongly that our mission is consumer reporting first and removal capability as a convenient (though important) feature.

Harms to computers/users from spyware -

- Changing browser or system settings - either upon installation or removal of the spyware: To what extent can this interfere with a consumer's ability to use their PC?

There are several issues here that should be explored:

1) Malicious or damaging content - If the bundled content was designed to do harm, the impact on the user's ability to use their computer(s) is obvious. Aside from the implication that this was a virus/Trojan, the next level would be an application that could change a user's Dialup Networking. This could cause the user a significant amount of money if the changes employ long distance and/or paid service.

2) System instability - Many of these applications can cause Operating system issues, browser instability, software conflicts, Boot and/or shut down problems, slow internet connections, etc.

3) Annoyance, productivity loss, frustration, confusion, dissatisfaction with the Internet as a whole - The user becomes inundated with popups, home page hijacks where the user is unable to remove the changes, file association changes, slow

connections, intrusive and/or inappropriate advertising, etc. If the user becomes so disgusted with the Internet as a whole then a major purpose of their computer has become useless to them and the Internet community suffers as a whole.

- Use of consumer's computer resources (memory and CPU cycles): How severely does this interfere with consumer's ability to use his/her PC? And how can one know what - or exactly what piece of spyware - is causing lock ups or crashes? Are there any independent labs, anti-spyware companies or other companies doing testing in this regard?

This varies according to the application causing the issue. It can be anything from little to extreme impact. We take this into account as part of our research on current as well as new detection candidates and is a major consideration as to whether it should be included in our data base. This alone will not cause us to add an application but it plays a major role in our inclusion procedures.

- Usurping user's computer - to send spam, porn, participate in DDoS attacks: How prevalent is spyware that results in these harms? Does spyware of this type create the potential for consumers' PCs to be hijacked by terrorists? And if so, how concerned is Homeland Security about this risk?

The first part of the question deals with elements we consider to be part of our evaluation process to determine if the application being researched should be added to our data base.

It is known that today's Viruses and Trojans can create problems across international boundaries. With the fact that malicious coders use ideas that others have pioneered to distribute their content it is only a matter of time before we see these kinds of exploits being used by terrorists and criminals. Trackware however does not spread as quickly as viruses. And if it is revealed that terrorists use or have created a given trackware it is essential that Home Land security and other international governmental agencies take note and pursue those responsible especially if the trackware is used to generate funding for the illegal activities of the terrorist or criminal organizations.

- What are the other security problems caused by spyware (e.g., opening up insecure ports to hackers, or as a result of just plain poor coding; opening a doorway to download and execute any program in the future on a consumer's PC; etc.) - and how prevalent are they?

Some applications utilize methods to prevent their removal, such as running duplicate processes, each watching over the other, to ensure that when one is terminated, it is quickly reloaded and executed. Also, some will download additional content for installation and execution, and if only one of the items is removed, the other may notice and therefore re-download and install this removed content, thereby causing a "re-infection" of the user's system. The security issue is that this content could be transmitting information, and attempts to terminate this are unsuccessful.

For applications which register themselves to the operating system, the files become protected by the OS. This prevents simply removing the file, as the OS will prevent the removal of a protected file (a file which is in use by the OS). This prevention is designed to ensure system stability (a.k.a. preventing removal of vital files required by the OS to operate), but is being exploited by items to aid in remaining on the system. Also, since these files are running concurrently with the OS, they are not visible from the user's perspective (there is no indication that they have executed and are now loaded in memory and running). Process viewers are required in order to find such items in execution.

There are a few which adjust associations of key file extensions, such as the EXE file extension, such that when *any* file with the .EXE extension is executed, the item which adjusted this association is FIRST executed, and in turn this executes the intended file. The issue is if the item which changed this association is removed, but the association is not adjusted back to the default setting, will cause all EXE files to be non-executable. The remedies which can be realized are to 1) put back the item which intercepts EXE file executions, thereby allowing for their operation, and then adjust the file extension and THEN remove the item, or 2) adjust the file association. Number 2 is difficult at this stage, as the item required (the registry editor) is in itself an EXE file, and therefore cannot run. The file extension can be changed to .COM instead of .EXE, and then executed successfully, and therefore allow for making the change, but in many cases, the item which changed the EXE association has also changed the COM association, thereby making that option also impossible to follow. The file extension infection is rare, compared to everything else, and is mainly performed by viruses, Trojans, and worms, and not by tracking items.

Some items monitor where users are traveling on the Internet. This could include Intranet addresses which contain secured information, or in the case of some web sites, the URL could contain personally identifiable information. This information could be transmitted and stored at the data-gathering company's servers, and used to link web usage information to personally identifiable information.

- Harm and costs to business - from dealing with tech support issues, cleaning spyware off corporate machines, AND - interference with a business's relationships with its customers as a result of spyware re-directing customer inquiries, spoofing the company, etc.

This can be very damaging in terms of technical support issues, transmission of company data, and with a company's reputation. With a possibility that proprietary/protected information could be transmitted to third parties, increased cost of technician call outs and/or system repair time, down time on essential company resources, problems with the ability to send and receive timely e-mail communications due to poor internet performance or the clogging of inboxes with viruses, bounced mail messages, and spam.

The spoofed e-mail could cause Internet service and filtering solution providers to cause mail from said company to be rejected. This alone can cause delays in technical support replies, essential intra/inter-business communications to be dropped, and consumer frustration as they perceive that their inquiries are being

ignored. Business relies on efficient and clear communications. If anything interferes with this, a company can and does lose customers as a result.

Turning to technological solutions issues:

- How does spyware get installed via "drive by"? And how much of a role does file sharing software (like KaZaA) play in spyware distribution - and does spyware distributed via file sharing programs involve unique security concerns? What about distribution by consumers' sharing files over file sharing systems?

Most "drive-by" installations are performed when a user visits a webpage with instructions to install something via ActiveX. This implies the user is viewing the page with Microsoft's Internet Explorer web browser. Depending on the user's security settings, the install instruction can be ignored (if ActiveX is turned off), it can prompt for the install (when ActiveX is set to Prompt, the most common setting), or it can install automatically (when the setting is set to Allow). Some items can adjust this setting to Allow, thereby allowing items to install without a user's knowledge.

While there is no clear definition of a "drive-by" install, many accept its meaning to be when an ActiveX prompt is presented asking for permission to install. Many users, when presented with an onslaught of popups and etc, will click without really reading in order to rid the screen of the unwanted prompt. Some users will simply click Yes when presented with a choice in an attempt to rid the prompt from the screen.

Concerning P2P software, many free P2Ps require agreeing to install such items in order to use the software. There are some, however, such as Grokster, which will install items even when the EULA (which states these terms) is **NOT** agreed to. In other words, even though the user does not accept the terms of the EULA, and exits the installer, some items still do install, without the user's knowledge.

P2P networks are more of a breeding ground for viruses and Trojans than tracking items. However, these types of items can still be distributed via P2P networks, especially if the program is masked as a download for one program, but in fact installs the unwanted items instead.

- Could protocols/settings/etc. - concerning the use or handling of BHOs, ActiveX, Java, etc. be changed?

These technologies are very important to the structure and development of the Internet. While making adjustments to these items could aid in stopping **some** items from being installed unexpectedly, there still remains many other methods that could be used. Restricting the installation of BHOs, ActiveX items, Java, etc. may be more hindering to the growth of these technologies than aiding in any overt prevention of a recognized exploit.

However, the use of managing software for these technologies would greatly enhance protection in this field. For example, there already exist third party managers for BHOs which a user can use to view what BHOs are installed and offers a method to remove them. If these functions were built in to the web browser, along with an easy way for the user to view and understand the information, it could enhance the removal of such items.

There could also be better management of these technologies. When an item wants to install, there should be much more information than is currently displayed. For example, when an ActiveX prompt appears, it usually does not indicate much about what the installation is for. Expanding the required information and greater flexibility over the options available when presented with such a prompt would benefit users. Instead of only having a selection box for trusting all software by a particular vendor, it could have a selection box to not trust software from the vendor, thereby eliminating the prompt for that company from appearing in the future. This is currently being addressed by Microsoft in their SP2 update in development.

However, it must be understood that in any approach taken, it is only a matter of time before methods are found and utilized to circumvent these efforts, thereby nullifying what has been attempted. Ultimately it is the user who can circumvent their own security through impatience, apathy, and lack of understanding. Awareness is the key to security and privacy and it is essential that the user take the time needed to read the EULAs, privacy policies, and installation warnings.

- Could anything be changed about the way the browser or operating system works to better deal with spyware?

The Windows Operating System is very flexible and configurable. This leads however to some serious drawbacks that could (in some cases) result in the OS becoming less secure, but restricting the operating system could adversely effect other applications that are currently installed on the user's system. We are daily made aware that many users do not make use of restricted or limited user accounts for every day use.

Regarding the browser the issue comes down to usability. Adding more security will block users from accessing the web pages and the functionality that they have come to expect. The best method would be to educate users about security/privacy and the limitations of their chosen applications.

- Could the protocols, handling, or anything else associated with display or contents of the download alert dialogue box - or with Trusted Certificates - be changed to resolve spyware problems?

Yes, this can and should be changed to give the user clear and understandable information about any content that might be installed on their systems. The fact remains though that security and privacy begin and end with the user. If the user does not take the time to understand the software and said information, the fact that notices and/or Trusted Certificates are there in no way implies that the user has read or even understood them.

- Could/should spyware be filtered - by ISP or users (a la spam?) There's also been some talk of blacklisting sites that allow drive by downloads (again, a la spam fighting techniques), or developing white listing techniques aimed at the installation/downloading of the spyware itself. What are the limitations or possible downsides of these solutions?

ISPs can provide this at the customer level. So that every user has the ability to say no to trackware, but can also to allow it should they so choose. There are of course many solutions available to implement this, but we should keep in mind that not all trackware will or should be

stopped. Encryption and bundled trackware is impossible to stop at a gateway level. To prevent the problem completely ISPs must license their own software as a browser to the end users so they can aide the user to take control of their internet connection.

- How do spyware blocker programs work - and how effective are they?

This is a very dangerous question and one we can not answer. If we were to reveal our or others methodology for achieving this, those who create the applications we and others detect, block, etc could use that information to defeat antitrackware solutions. Though we do recognize that eventually these developers will discover a way to defeat any given detection, blocking, and/or removal technology, we do not want to make it easy for them to do so.

The effectiveness and/or relevance of any given antitrackware solution ultimately depends on its performance. The only one who can determine this is the end user themselves by actually using the solutions available and from this making a personal decision as to whether it is the "right" solution for them.

- Are there other ideas for technological means of dealing with spyware?

Yes, the following are some useful suggestions to explore:

- Server based computing with thin clients can allow central control of security in the end user's computing environment. This would keep the content in a central location and thus not affect the system being used by the end user.
- Licensing elements of the ISP's software can enable service personnel to remotely manage the end user's system (with the user's permission of course as part of an overall technical service contract).
- Improvements in controls that would allow the user to more easily manage installed components such as BHOs, ActiveX, and Alternate Data Streams (ADS).

Michael A. Wood
Sales Director USA and Canada
Lavasoft
Nicolas Stark Computing AB
Tel (US) (919) 499-6663
FAX (US) (919) 499-6683

Lavasoft
Nicolas Stark Computing AB
Centrumvägen 39 | Box 80 | 52043 Åsarp, Sweden
Phone: +46-51550300
Fax: +46-51553019
www.lavasoft.de |
www.lavasoftsupport.com