

Anti-Spyware Coalition

Summary of Comments and ASC Response on the October 27, 2005 Draft of the *ASC Risk Model Description*

Summary

The Anti-Spyware Coalition (ASC) received over 100 comments from the public during the 30-day comment period for the first draft of its Risk Model Description document. The ASC is grateful to the many organizations and individuals that participated in the public comment process. The coalition incorporated many of the suggestions offered by public into the final Risk Model Description Working Report.

The substantive comments on the description generally fell into four categories: 1) those praising the ASC for creating a Risk Model Description; 2) those offering general criticisms suggesting that the very existence of a Risk Model Description with differing risk levels is counter-productive to protecting users; 3) those offering general criticisms suggesting that the ASC has not gone far enough in providing specific guidance for anti-spyware vendors; and 4) those offering specific suggestions to improve the Risk Model Description.

None of the broadly critical comments offered other suggestions for other means to achieve the main goal of the Risk Model Description: making the decisions of anti-spyware vendors more transparent while continuing to provide a vibrant marketplace of tools to protect consumers and enterprises. ASC continues to believe that the Risk Modeling Document is an important next step toward this goal.

The more specific suggestions greatly aided the ASC in improving the document. In particular, many comments pointed out that ASC was using the same “Risk Level” ranking for both “Behavior That May Impact Users” and “Consent Factors,” despite the clear intent that the two elements counter balance one another as opposites. The final working report addresses this issue by clearly differentiating between risk levels (negative) and consent factors (positive) in the overall risk modeling process. Most of the other substantive comments addressed specific objective criteria.

Contents

ASC divided the comments received over the past month into four substantive categories:

- 1) Praise for the Risk Model Description
- 2) General criticisms suggesting that the very existence of a Risk Model Description with differing risk levels is counter-productive to protecting users
- 3) General criticisms suggesting that the ASC has not gone far enough in providing specific guidance for anti-spyware vendors
- 4) Those offering specific suggestions to improve the Risk Model Description

- Comments Regarding Personal Information
- Manual Steps of Uninstallation
- Uninstallation of Bundled Components
- Definition of “Software Components”
- Unwanted Behavior
- Consent and EULA Concerns
- Hijacked Browsers and Settings Concerns
- The Potential for False Positives
- Software Packers and Installers
- Terminology
- Cumulative Nature of Risk Criteria
- Individual Risk Criteria Suggestions

ASC Also received non-substantive comments that included:

- Complaints about ASC Members
- Comments on the ASC Definitions Document

Praise for the Risk Model Description

ASC received a number of comments that contained general thanks and encouragement. These comments required no substantive response from the Coalition but were greatly appreciated and helped to confirm what the ASC believes is broad-based public support for the Coalition’s anti-spyware efforts.

Risk Model Description Does Not Help Protect Users

ASC received a large number of comments, mostly from individuals, suggesting both that the Risk Model Document does not fully address the problem of spyware and that it does not go far enough to protect users. Most of these commenters demanded that no software be granted unauthorized access to their computers and opined that nearly all of the behaviors laid out in the document should carry a “high” risk rating. Some of these comments focused on the importance of user consent to installation. Many comments expressed the opinion that the risk definitions for installation with minimal consent were too low and should be raised. For example:

“I am concerned that you do not consider activities that will modify my computer without asking my permission as not being spyware or low risk. Anything that modifies my computer without my express permission is high risk regardless of the intention.”

(Anonymous)

These comments, while numerous, did not provide many concrete suggestions for modifying the Risk Model Description. ASC is sympathetic to the concerns of these users, however it is important to remember that 1) this document is only part of a complete solution to the spyware problem, which includes technology, enforcement and education, and; 2) most reputable anti-spyware vendors already have criteria that they use

to make objective decisions. ASC is not requiring anti-spyware vendors to act in a particular way in any instance. The Risk Model Description is an attempt to harmonize these various criteria and publish them in order to provide transparency.

Risk Model Description Does Not Provide Enough Guidance to Anti-Spyware Vendors

ASC also received a number of comments, mainly from individuals or organizations involved with advertising companies expressing concern that the Risk Modeling Document is not specific enough to provide suitable guidance for anti-spyware vendors when they create spyware definitions.

The Risk Model Document is only one part of the Coalition's broader anti-spyware effort and is not intended to homogenize all vendors' spyware definitions.

These comments also raised the issue of a lack of a "Best Practices" document from ASC that could provide further guidance to anti-spyware vendors. As ASC has indicated in the past, the Coalition does intend to create a best practices document in the future. The Coalition is also pleased to see the results of the TRUSTe best practices document. All interested parties are encouraged to participate in the ASC public meeting on February 9, 2006.

Specific Suggestions to Improve the Risk Modeling Document

ASC received a smaller number of comments with specific suggestions to improve the document. Most of the changes that ASC has made for the final working draft came from this subset of comments.

- **Comments Regarding Personal Information**

ASC received comments from readers who were concerned with the handling of users' personal information. One comment from an advertising trade association disputed the use of the term "loss" with regard to a user's personal info, preferring the term "misuse" as a better descriptor. ASC believes that the distinction is not meaningful to consumer or enterprise users. It matters little to consumers whether their personal data is merely lost or actively misused. In either case consumers are forced to assume the worst, and take proper steps (putting a hold on a credit report, contacting the Social Security Administration, etc.) to protect their personal data. Because consumers and enterprise users are the customers of anti-spyware software, the guidelines must assume the worst as well.

Also regarding personal information, some writers commented that the term "arbitrary data" is not defined in the document, although it is used a number of times. There was some concern that this lack of a definition may lead to an overly broad reaction to programs that did not cause a specific harm to the user's personal information. This data is only a concern to the ASC in that there is some likelihood of personal information being lumped in by that chance. Again, our

guidelines must assume the worst in these situations in order to be helpful to consumers and enterprises. ASC made a small change to address this issue.

- **Manual Steps of Uninstallation**

It was brought to ASC's attention that the term "manual steps," as used in the "Removal" section of the Document was an overly broad construction. The simple act of opening the Add/Remove Programs control panel or executing an uninstaller could be considered a manual step. ASC has changed the Document to read "tedious or unusual manual steps" in an effort to clarify the intent of the section.

- **Uninstallation of Bundled Components**

A few comments suggested that the uninstallation section of the Risk Modeling Document was not clear enough about the removal of bundled software components. ASC clarified the language in the section to make it clear that uninstallers should offer to remove all of the software that was installed.

- **Definition of "Software Components"**

There was concern expressed in some comments that the term "software components" was not defined clearly enough, and could refer either to separate software programs downloaded simultaneously or to individual files within one piece of software. It was not ASC's intention to suggest the second definition. We are only concerned with multiple applications being installed at once. The document has been changed to reflect this.

- **Unwanted Behavior**

One commenter raised a concern in some of the comments received that ASC's usage of the term "behavior" as unwanted was confusing. ASC has attempted to make it clear that the behaviors described are exhibited by certain technologies making them potentially unwanted by users. It is always the user's decision whether a certain technology is wanted or unwanted. Based on the comments, ASC made some minor changes to the Final Working Report to ensure that this philosophy is clear and consistent throughout the document.

- **Hijacked Browsers and Settings Concerns**

A few writers had concerns about the low or medium risk designations given to behaviors such as changing settings in web browsers or the system at large, as well as the semantic difference assigned to "spyware" versus "adware." The writers felt that the time involved in cleaning the system of adware and the potential for children to be exposed to adult advertisements because of an infection warranted a higher risk rating for these behaviors.

- **The Potential for False Positives**

A small number of comments expressed concern that some legitimate software could be marked as spyware, even while being used in the intended manner.

“Please also be sure to require a distinction to be made for programs that would normally be considered acceptable, but happen to be sometimes bundled and deployed by spyware in unacceptable (sic) manners (without the consent or control of the software’s original developers).”
(Jeff Lawson)

As ASC has said before, this is an important concern that anti-spyware companies should be attentive to in their vetting process.

- **Software Packers and Installers**

Several other comments raised in the Risk Modeling Document regarding the use of programs such as “packers” were disputed by companies who used them to protect their own software from decompilation and reverse engineering. They believed that such protection of software should not be considered a risk factor. The position of ASC in this matter is that risk in this case is predicated upon consent. The user should be informed about the intent of the packer and the packer should follow the guidelines for uninstallation of all of its components.

- **Terminology**

In general, these comments focused on the labeling (extortionware, junkware) and what is called spyware versus adware. The ASC’s intent in creating the Risk Modeling Document was to offer guidelines for detecting and removing spyware. Although many labels can be applied to software that users find objectionable, this document is focused on establishing guidelines to detect and remove it.

- **Cumulative Nature of Risk Criteria**

A few comments received were in regard to the overly broad categorization of a number of criteria, such as the “Runs Without Explicit User Consent” and “System Integrity” sections. The complaint was that there are many programs that run without explicit consent or that can cause system instability, but that does not have a bearing whether or not their behavior is potentially unwanted, and they should not necessarily be removed from a user’s computer because of it. ASC understands these concerns, but wishes to point out that these criteria are cumulative in their applications. A program causes some system instability but which is otherwise a harmless or useful application should not be flagged as spyware. Similarly, a program that launches at startup without explicit consent could be benign. It is only when these behaviors are combined with other risk criteria does it become more likely that the application in question will be categorized as spyware.

- **Individual Risk Criteria Suggestions**

ASC received a small number of other comments that exclusively modified individual risk criteria to change assigned risk levels. The Risk Modeling subgroup reviewed these suggested changes and applied them as needed.

Non-Substantive Comments

- **Complaints About ASC Members**

As with the Definitions document, a small number of people suggested that ASC lacked credibility simply by virtue of the members of the Coalition. None of these comments had constructive criticism to offer, and therefore required no response from ASC.

In many cases these comments alleged that certain ASC members offered products that were spyware or contained spyware. The ASC is not a policing organization and exercises no control over its members' internal practices. Each member of the coalition has been approved by the others as a legitimate anti-spyware software vendor, distributor, academic or consumer interest group. Individuals with complaints against any organization should contact the company in question.

There were a few comments directed at anti-spyware vendors as a whole that suggested the anti-spyware industry was exaggerating the threat to users, especially from tracking cookies, in order to boost their own sales. Polls taken before and after the advent of anti-spyware software, have consistently shown that Internet users are very concerned over the rapid advance of tracking technology on Internet connected computers even in cases where very little data about them is compromised. In addition, ASC hopes that different anti-spyware vendors will offer different levels of protection so that users will be able to choose how they would like issues such as tracking cookies are addressed. The Risk Model document specifically suggests that companies that do make decisions about tracking cookies should make that very clear to users that they are doing so in order to help users that would like to keep these tracking cookies aware that they may wish to use another product.

- **Comments on the ASC Definitions Document**

During this comment period, there were a number of people who submitted comments related to the Final Report of the ASC Definitions document. While ASC is no longer officially taking comments on this document, we do encourage individuals to submit comments on all ASC documents. The Coalition will continue to review all of these comments and make updates as appropriate.