

Anti-Spyware Coalition Risk Model Description

Introduction

The anti-spyware industry offers a robust selection of tools to consumers in the marketplace. As is to be expected in such an environment, the rating systems used to classify Spyware and other Potentially Unwanted Technologies vary between Anti-Spyware vendors. The members of ASC believe that reputable anti-spyware companies should be transparent about their decisions to help users understand how anti-spyware tools make decisions; software publishers understand what may concern users; and Anti-Spyware vendors share information about emerging threats.

To facilitate that transparency, the ASC has developed a list of a broad set of behaviors that its members can use to help users make decisions. We expect the list to change over time as new bad practices are discovered.

Goals

This document will:

- Outline the common terminology and process for classifying potentially unwanted technologies
- Describe the behaviors that can lead to detection so that software vendors and users will have a better understanding of the decision-making process
- Provide an overview of the approaches used to classify a software application

The risk modeling system is based on behavior. The risk and consent factors described below lay the groundwork for the eventual publication of industry-wide Best Practices.

Ultimately, the decision on what rating to give and what risk model to use falls to the individual Anti-Spyware vendor. This decision was intentional, to give each vendor the flexibility to rate software on their own terms while agreeing to a common framework.

Anti-Spyware vendors agree on the basic terminology and factors leading to risk or consent, but will differ on the exact modeling system and thresholds for detection. The variations in modeling help users make better marketplace decisions by selecting products that align with their priorities. The common framework and language regarding risk and consent behaviors helps Anti-Spyware vendors describe their models consistently, and gives standard guidance to application vendors about the factors that may lead to a program being flagged.

The criteria below outline the key factors that members of the Anti-Spyware Coalition use to make a determination – vendors may decide to use all or a subset of the criteria. In general, a program’s rating will increase with risk behaviors, and decrease with behaviors that provide user consent and control.

Modeling Process Overview

The risk-modeling process is the method Anti-Spyware vendors use to determine the classification of a program. Members of the Anti-Spyware Coalition use the same essential modeling process:

- Determine the installation method used
- Install and research software to determine areas of impact
- Measure the risk factors
- Measure the consent factors
- Weigh the risk factors against the consent factors to determine what classification and level apply, if any

While Anti-Spyware Coalition members agree on the factors that increase risk or consent, each member weighs and combines these factors on their own scale. Although ratings should not differ greatly, variations are possible because Anti-Spyware products have differing foci and philosophies.

For example, one vendor may not detect a program that tracks the user if such behavior is turned ‘off’ by default, while another may detect such a program but at a low warning level.

Overview of the Risk Categories:

Spyware and other Potentially Unwanted Technologies encompass a wide variety of behaviors that can concern users. To help understand the impact, we can describe software as affecting one or more of the following areas:

Privacy – Compromising the user’s information or data, such as

- Exposure to fraud or identity theft
- Loss of personal information
- Unauthorized tracking

Security – Impacting the system integrity of the computer, such as

- Attacking the computer, or using it as part of an attack
- Exposing the computer to risk by lowering security settings
- Using computer resources in an unauthorized manner
- Hiding programs from the user

User Experience – Impacting the user’s functionality of the computer, such as

- Delivering unexpected advertisements
- Changing settings
- Creating system instability or slowing performance

These risk categories are not mutually exclusive, and are not limited to the examples above. These represent the general areas Anti-Spyware vendors examine, and help describe the impact to users in common terms.

For example, a program may be detected by an anti-spyware vendor because it intercepts network traffic. The anti-spyware vendor may wish to explain this as an impact to privacy, rather than explaining the details of the underlying technology (which may be described in a more extensive write-up).

To further describe a program, some Anti-Spyware vendors may choose to rate a program along each risk category, while others may merge the categories into a single rating.

Risk and Consent Factors

Many applications have complex behavior – the final determination of a program requires a judgment call on the part of the Anti-Spyware vendor, based on their policies about what programs should be brought to the user's attention. The following are key considerations in the risk modeling process:

Technologies/Activities are neutral

- Technologies and activities like data collection are neutral, and as such are harmful or helpful depending on their context. Anti-Spyware vendors need to consider both the factors that increase risk and the factors that increase consent before making a determination.

Many risk factors can be mitigated

- A risk factor is an indication that a program has certain behavior. The Anti-Spyware vendor must consider this behavior in context and decide whether the consent factors mitigate the risk. Some risk factors may not flag a program on their own, but could be considered in combination with other factors. Certain risk factors are impactful enough that they cannot be mitigated, such as installation by security exploit. The Anti-Spyware vendor may choose to always alert the user about programs with this behavior.

Weights can differ

- Anti-Spyware vendors may weigh behaviors differently, depending on their policies about what behaviors are taken into consideration. Each vendor sets their own threshold for detection based on the weights they assign to the risk and consent factors.

Strive for objective, consistent rules

- The factors outlined below are meant to be objective and easy to apply consistently. However, certain factors cannot be determined programmatically but are still important to users (such as the use of deceptive text or graphics). In these cases, each Anti-Spyware determines the impact according to their internal policies.

The common agreement in the Anti-Spyware Coalition centers on what factors increase risk and what factors increase consent. Therefore, the general advice for an application vendor is to

- Minimize the risk factors
- Maximize the consent factors

The lists below cover a wide variety of behaviors, and are not exhaustive. They will grow with time as new behaviors emerge.

Risk Factors

The following risk factors are behaviors that have the potential for user harm or disruption. In some cases, the behavior may be desired, such as data collection for personalization, but can still present a risk if unauthorized. Many of these risks can be mitigated by providing the appropriate consent factors.

In certain cases, a risk may be serious enough that a vendor may decide to inform users, even if consent was given. This may be the case for certain monitoring or security tools (users who knowingly install such programs can dismiss these warnings). Other risks, such as “installing by security exploit” may warrant automatic detection, no matter what other consent was given.

Some risk factors may be minor, and not enough to warrant detection on their own. However, the low-risk behaviors can help differentiate two similar programs, or may be combined into a higher risk level if enough low-risk behaviors are present. Anti-Spyware vendors may use confirmed user feedback, Terms of Service agreements, EULAs or privacy policies as a part of their investigation into a risk factor.

We rate and classify software based primarily on behaviors inherent in the software itself. Note that installation method varies not only from program to program, but also by the distributor of the software and in some cases even by distribution model. In cases where intrusive, covert or exploitative installation has been observed, this fact is taken into account by each Anti-Spyware vendor according to its policy.

The risk factors have general weights (High, Medium and Low) that help show the relative impact to the user. Although all behaviors can be problematic if unauthorized, certain ones tend to have a greater impact and are treated with more

severity than others. Clearly, the impact can vary if a behavior is performed repeatedly, is combined with other behaviors, or occurs with varying levels of consent.

The list below is a combined set of the behaviors that members of the Anti-Spyware Coalition consider in their analysis. Each Anti-Spyware vendor weighs the behaviors as they see fit in their modeling formula.

Behavior that may impact users / Relative Impact

Installation & Distribution, including but not limited to:

- Replication behavior (mass-mailing, worming, or viral) *High*
- Installs without user's explicit permission or knowledge, such as not providing or ignoring user's request to cancel installation, drive-by installation, use of a security exploit, or software that meets other risk factors and is undisclosed in a software bundle (Note: The rating of High indicates a typical rating for this item and its relative risk. The specific weight may vary depending on the impact and/or number of items installed.) *High*
- Uninstalls other applications, such as competitive programs *High*
- Software updates automatically *Medium*
- Program downloads, is bundled with or installs software that has potentially unwanted behavior, as described in definitions document (Reminder: The rating of High indicates a typical rating for this item and its relative risk. The specific weight may vary depending on the impact and/or number of items installed.) *High*

Identification & Control, including but not limited to

- Has incomplete or inaccurate identifying information *Medium*
- Program obfuscated with tools that make it difficult to identify, such as a packer *Medium*
- Creates polymorphic or randomly named files or registry keys *Medium*
- No indication the program is running inside an application, such as an icon, toolbar or window *Low*
- No indication the program is running standalone, such as a taskbar, window or tray icon *Low*
- Previously installed program runs automatically without explicit user consent *Low*

Networking, including but not limited to:

- Proxies, redirects or relays the user's network traffic or modifies the networking

stack *High*

- Creates or modifies “hosts” file to divert domain reference *High*
- Changes default networking settings (Broadband, telephony, wireless, etc.) *High*
- Dials phone numbers or holds open connections without user permission or knowledge. *High*
- Alters the default internet connection to connect at a premium rate (i.e. 2x normal rate) *High*
- Sends communications including email, IM, and IRC without user permission or knowledge *High*
- Floods a target with network traffic *Medium*

Data Collection, including but not limited to:

- Transmits personally identifiable data (Reminder: Technologies are neutral, and only a concern when abused. A behavior can be acceptable with notice and consent). *High*
- Collects personal information, but stores it locally *Medium*
- Intercepts communication, such as email or IM conversations (Reminder: Technologies are neutral, and only a concern when abused. A behavior can be acceptable with notice and consent). *High*
- Uploads arbitrary data, some of which could be personally identifiable *Medium*
- Uploads data that can be used to track user behavior offline and online as well as other types of data that may be sensitive, yet not personally identifiable *Low*
- Uses tracking cookies to collect information (Reminder: Each Anti-Spyware vendor weighs a behavior according to their own policy. ASC recommends that vendors that utilize this criteria make it clear to users that they do so, affording users the opportunity to make an informed marketplace decision) *Low*

Computer Security, including but not limited to

- Hides files, processes, program windows or other information from the user or system tools *High*
- Denies access to files, processes, program windows or other information *High*
- Allows remote users to alter or access the system (files, registry entries, other data) *High*
- Allows host security to be bypassed (privilege elevation, credential spoofing, password cracking, etc.) *High*
- Allows remote parties to identify vulnerabilities on the host or elsewhere on the network *High*
- Exploits a vulnerability on the host or elsewhere on the network *High*
- Allows remote control over a computer, including process creation, spamming,

- or attacks on third parties *High*
- Disables security software, such as AntiVirus or Firewall software *High*
- Lowers security settings, such as in the browser, application, or operating system *High*
- Allows for remote control of the application, beyond self-update *High*

User Experience, including but not limited to:

Advertising

- Displays external advertisements that are not attributed to their source program (this does not cover advertisements created by online content users deliberately visit, such as web pages) *High*
- Displays external advertisements that are indirectly attributed to the source program (such as a pop-up with a label) *Medium*
- Displays external advertisements that are clearly attributed to the source program, such as starting alongside the program *Low*
- Replaces or otherwise alters web page content, such as search results or links *High*

Settings

- Changes files, settings or processes to reduce user control. *High*
- Changes browser pages or settings (error page, home page, search page, etc.) *Medium*
- Modifies user settings such as favorites, icons, shortcuts, etc. *Low*

System Integrity

- With other risk behavior, potential to cause frequent system instability *Medium*
- With other risk behavior, potential to use excessive resources (CPU, Memory, Disk, Handles, Bandwidth) *Medium*
- Attaches to other programs, such as the browser, using a non-standard method *Low*
- Disables or interferes with functionality of system (right-click behavior, ability to use system tools, etc.) *High*

Other Behaviors, including but not limited to

- Has other potentially unwanted behavior, as described in definitions document *Medium*
- Program modifies other applications. *Medium*
- Program generates serial numbers/registration keys. *Medium*

Removal, including but not limited to

- Self-healing behavior that defends against removal or changes to its components, or requiring unusual, complex or tedious manual steps to run the uninstaller *High*
- Uninstaller does not functionally remove the program, such as leaving components running after reboot, not offering to uninstall bundled applications, or silently reinstalling components *High*
- Does not provide an easy, standard method to permanently stop, disable or uninstall the program (such as Add/Remove Programs or equivalent). *High*
- Uninstaller repeatedly attempts to badger or coerce the user into cancelling the uninstall *Low*
- With other risk behavior, does not offer to uninstall bundled or subsequently installed software components. *High* (Reminder: The rating of High indicates a typical rating for this item and its relative risk. The specific weight may vary depending on the impact and/or number of items installed.)

Non-Programmatic Behaviors, including but not limited to

- Contains or distributes offensive language and content (Reminder: Each Anti-Spyware vendor weighs a behavior according to their own policy. ASC recommends that vendors that utilize this criteria make it clear to users that they do so, affording users the opportunity to make an informed marketplace decision) *Medium*
- Consists of advertising components and is installed at or through web sites designed for, targeted at, or heavily used by children 13 and under *Medium*
- Uses misleading, confusing, deceptive, or coercive text or graphics text, graphics, advertising or other false claims to induce, compel, or cause users to install or run the software or take actions (such as click on an advertisement) *Medium*

Consent Factors

The behaviors below indicate that a program provides users with some level of notice, consent and control that may help mitigate a risk factor. Certain high-level risks may be extensive enough that no level of consent can mitigate them, and the Anti-Spyware vendor will always warn users about such behavior.

The consent factors help lay the terminology and groundwork for Best Practices, which is a set of positive examples that demonstrate clear notice and consent. (Note: The Best Practices will live in a separate document, based on the final version of this document.)

It is important to note that these consent factors are per-behavior. If a program has multiple risky behaviors, each is examined separately for its consent experience.

The weights (Level 1, Level 2, Level 3) indicate a relative ordering for the consent behaviors – although all are helpful, some behaviors provide more consent than others. Again, each Anti-Spyware vendor can weigh the characteristics on their own scale based on the level rating and their understanding of the particular case. As with the behaviors that may impact users, these factors should be seen as cumulative. Level 1 represents less active consent while Level 3 represents the most active and, therefore, highest level of consent.

In the list below, the term “Potentially Unwanted Behavior” refers to any program activity or technology that can present a risk to users if abused, such as data collection or changing system settings. These technologies are described in more detail in the definitions document on the Anti-Spyware Coalition website.

Behavior that provides user consent / Level of Consent

Installation & Distribution

- Distributed via download, in clearly labeled packages, and not bundled by affiliates *Level 3*
- Requires high level of consent before installation, such as registration, activation, or purchase *Level 3*
- Has clear, explicit setup experience that users can cancel *Level 3*
- Potentially unwanted behaviors are clearly called out and prominently disclosed outside of EULA *Level 2*
- Potentially unwanted behaviors are part of the expected functionality of the program (i.e., an email program is expected to transmit information) *Level 3*
- User can opt-out of potentially unwanted behaviors *Level 2*
- User can opt-in for potentially unwanted behaviors *Level 3*
- Obtains user consent before software updates *Level 3*
- Obtains user consent before using passive technologies, such as tracking cookies *Level 3*

Bundled Software Components (separate programs that will be installed)

- All bundled software components are clearly called out and prominently disclosed outside of EULA *Level 2*
- User can review and opt-out bundled components *Level 2*
- User can opt-in for bundled components *Level 3*

Visibility (Run-Time)

- Files and directories have clear, identifiable names and properties in

accordance with industry standards (Publisher, Product, File Version, Copyright, etc.) *Level 1*

- Files are digitally signed by publisher *Level 2*
- Program has a minor indication when it is active (tray icon, banner, etc.) *Level 2*
- Program has major indication when it is active (application window, dialog box, etc.) *Level 3*

Control (Run-Time)

- Sponsor programs only run when sponsored program is active *Level 2*
- Clear method to disable or avoid program, aside from uninstall *Level 2*
- Program requires explicit user consent before starting (i.e., double-click an icon) *Level 3*
- Program has opt-in before starting automatically *Level 3*

Program Removal

- Provides straightforward, functional uninstaller in well-known location (such as Add/Remove Programs) *Level 2*
- Program uninstaller removes all bundled components *Level 2*

Conclusion

The consent factors, risk factors and modeling process outline the analysis approach used by members of the Anti-Spyware Coalition. Although behavior weights may vary between vendors, the core guidance for application developers is to minimize the risk factors and maximize the consent factors to avoid classification. However, certain risks may be serious enough that an Anti-Spyware vendor will always inform users about impact of the behavior.

The risk modeling process is a living document, and will change over time as new behaviors and technologies emerge.