

Conflict Identification and Resolution Process

I. Introduction

This document is intended to provide voluntary guidelines within the Anti-Spyware industry to assist in avoiding and resolving conflicts between suites of Anti-Spyware software and to better serve consumers. The guidelines propose three main elements: the sharing of software versions so as to reduce or minimize conflicts, the provision of accurate information about conflicts to consumers, and the prompt response and cooperation between vendors to seek to resolve conflicts.

Although aimed at addressing conflicts among members of the Anti-Spyware Coalition (ASC), these guidelines can be used to address conflicts between any two anti-spyware vendors, by agreement between the vendors. If a conflict arises, for example, between software produced by an ASC member and the software of a non-ASC member, the two companies can choose to use these guidelines (or a modification of the guidelines). Anti-spyware vendors that are not ASC members are welcome to contact individual ASC members directly to inquire about the information and code-sharing suggested below; each ASC member will maintain their own criteria for applying these guidelines to non-ASC members.

A. History of Security Software and Conflicts

In the early days of the antivirus industry, technical conflicts resulting from the installation of two or more antivirus products on the same computer were not uncommon. Typically, such conflicts were easily identified and resolved in a collegial manner, with little, if any, formalized process.

As technology has evolved to include more real-time detection technologies and complex, system-wide removal routines, resolution of some of these issues has become more complicated. Conflicts can now involve two programs attempting to use one resource, or attempting to perform identical functions. In such cases, the widely accepted best practice has been for products to alert users when technical conflicts arise, allowing users to decide whether or not to proceed with installations that could render existing programs unusable, or that could result in a newly installed product not functioning as expected.

Absent any standard procedure for resolving disputes, many of these increasingly complex conflicts have simply gone unresolved. Although there are several industry mailing lists that allow vendor representatives to raise issues regarding conflicts, technical constraints made it impossible for some conflicts to be resolved. In cases where agreement cannot be reached the parties involved in conflicts have had to simply agree to disagree, to the detriment of users.

B. New Issues to Resolve in Anti-Spyware Space Due to Consumer Confusion and Marketplace Changes

Lessons drawn from the anti virus industry's traditional approach to conflict resolution must be applied to the Anti-Spyware field with care. Confusion regarding what is and is

not spyware, what behaviors ought to be off limits, and the gray areas surrounding advertising-supported software complicate matters of conflict between Anti-Spyware technologies.

Because anti-spyware companies cannot simply rely on what has worked before, the Anti-Spyware Coalition has drafted this document to serve as a framework within which companies may resolve software conflicts.

II. Guidelines for Reviewing and Addressing Conflicts

A. Introduction

ASC's role, and the role of this document, is to promulgate voluntary guidelines that companies can use to resolve conflicts amicably, to encourage the sending of accurate information to consumers, and to establish processes for the sharing of information and software to make for easier and earlier testing of software before it goes to the consumer.

B. Exchanging New Software Versions

In order to minimize and if possible avoid conflicts between products, software suites should be available to quality assurance teams of all participating ASC members.

ASC members should offer, free of charge, access to pre-release, public beta or full release versions of new security products or software suites to other participating members, so that conflicts between suites can be discovered and addressed before full public release of the software.

The license of the shared software should enable vendors to:

- Maintain a system or virtual machine (VM) image that contains a complete installation of the software and required updates;
- Install and uninstall the software as needed;
- Update the software and associated data (signatures, etc) as any regular user; and
- Update the software and associated data from a beta source from the vendor, should beta versions be available.

This sharing can be conditioned upon establishing a direct relationship including appropriate legal agreements.

Each participating company should provide ASC with contact information of the individuals responsible for maintaining direct relationships. The contacts should be able to provide, at minimum, copies of the most recent versions of available software as well as beta or pre-release versions, if possible. The contacts should be responsible for replying to all ASC requests in a timely manner.

The Anti-Spyware Coalition will provide a database of each company's contacts on a secure, members-only area of the ASC site. ASC will also maintain a mailing list that allows ASC members to contact each other regarding conflict resolution, access to protected public servers, or access to older versions of software not available on the public server.

C. Accuracy In Communications with Consumers Regarding Competing Products

A vendor that is claiming the existence of a conflict with the product of a second vendor must be able to demonstrate that such a conflict exists.

When a conflict does exist, a vendor should make all explanations offered as precise as possible while still presenting the information in a manner that average users can easily understand. To this end, references should be made to conflicts between individual elements* of a program.

Whenever possible, a conflict with a suite of Anti-Spyware software should be communicated by identifying the element of the suite responsible for the conflict. When communicating with users during installation or operation, an entire suite of programs should not be listed as conflicting when one small portion of the suite actually causes the conflict. Also, to prevent confusion among users, software should avoid identifying conflicts at a highly granular and technical level (although vendors should provide more detailed information if requested by a user). Communicating a conflict between two particular device driver files, for instance, is not likely to be of use to most consumers.

Once a conflict is identified to the user, the consequences of the conflict should be clearly outlined. These should include both the consequences of allowing the conflicting element to remain active on the system in question and the consequences of removing or disabling the conflicting element. When suggesting a resolution to the conflict, a vendor should strive to present the least intrusive methods of resolution possible.

D. Reasonable Response Time To Anti-Spyware Companies Seeking to Discuss Conflicts

The appropriate timeframe for investigating and resolving conflicts depends on the circumstances. The companies involved should work together in good faith to develop a solution and target timeframe that balances the user impact posed by a particular issue, versus the engineering challenges associated with investigating and remedying it. In some cases a technical resolution may not be possible. Within the agreed-upon timeframe, regular communications should occur between the two companies. Anti-Spyware companies should respond to initial inquiries from other Anti-Spyware companies regarding program conflicts within three (3) business days. Anti-Spyware companies should take a reasonable amount of time to address the investigation and remediation of program conflicts. Response time is dependent on several factors including, but not limited to:

- The nature of the conflict
- The pieces of software involved

* For the purposes of this document, an element of a program is defined as “a portion of a software program or suite that can be separately identified to the user.” For example, within a suite that contains a real time monitoring component and a user instigated scanning component, each component would be considered an element.

Anti-Spyware Coalition

- The potential impact on software suites
- The complexity of a particular program conflict.

Affected companies should provide mutual status updates every seven (7) calendar days, unless a different interval has been agreed to by both parties.

E. Limiting Conflicts

Anti-Spyware vendors should always consider providing consumers with choices where possible, such as the ability to turn off individual elements of a suite that may conflict with other suites during install, or disabling one feature of the suite permanently, for the purposes of limiting conflicts should they occur.

F. Signing Executables to Assist in Assurance of Authorship

Anti-Spyware vendors should always digitally sign their code with a certificate that becomes part of a chain of trust. Doing so allows other Anti-Spyware vendors to recognize and white-list pieces of code that belong to other vendors and which might otherwise conflict.