Intel Security Potentially Unwanted Programs (PUP) Policy

February, 2016

Intel® Security recognizes that legitimate technologies such as commercial, shareware, freeware, or open source products may provide a value or benefit to a user. However, if these technologies also pose a risk to the user or their system, then users should consent to the behaviors exhibited by the software, understand the risks, and have adequate control over the technology. Intel Security refers to technologies with these characteristics as "potentially unwanted program(s)," or "PUP(s)."

The Intel Security PUP detection policy is based on the premise that users should understand what is being installed on their systems and be notified when a technology poses a risk to their system or privacy. PUP detection and removal is intended to provide notification to our users when a software program or technology lacks sufficient notification or control over the software or fails to adequately gain user consent to the risks posed by the technology. McAfee® Labs is the Intel Security team responsible for researching and analyzing technologies for PUP characteristics.

McAfee Labs evaluates technologies to assess any risks exhibited by the technology against the degree of user notification and control over the technology. This process includes assessing the risks to privacy, security, performance, and stability associated with the following.

- **Distribution**: how users obtain the software including advertisements, interstitials, landing-pages, linking, and bundling.
- **Installation**: whether the user can make an informed decision about the software installation or add-ons and can adequately back out of any undesired installations.
- **Run-Time Behaviors**: the behaviors exhibited by the technology including advertisements, deception, and impacts to privacy and security.
- **Uninstall**: whether the user can easily remove all functional components of an install.

These areas are then evaluated against the following.

- **Notification**: the extent to which the user is notified of the software risks.
- **Consent**: the extent to which the affected users can consent to the software risks.
- **Control**: the degree of control that the user has over the software installation, operation, and removal.

Failure to meet all the criteria in this document will result in the technology being blocked by McAfee security products.

When objectionable distribution practices are used by a technology or its distributors, users (and antivirus scanners) may be unable to distinguish between compliant versions distributed using acceptable means and versions distributed using objectionable means. As a result, software that is distributed using objectionable practices may result in detection for other or all versions of the technology.

Any software that exhibits malware behaviors will not be tolerated and will be detected and removed as malware.

Distribution

Objectionable distribution methods can impair the overall user experience. Criteria for evaluating the distribution of software are as follows:

- Software must not be linked to or distributed using spam email.
- Software must not be distributed or installed by malware or by otherwise malicious (for example, drive-by) installations.
- Software installers must provide software licensing information prior to the installation of any bundled components.
- Software installers must inform users when the installation of bundled components are required for the installation of the main technology (that is, not optional).
- Software installers must allow the user to cancel the installation of all components if the installation of any bundled components is required for the installation of the main technology.
- Software installers must provide consistent (for example, Accept/Decline) options when offering one or more bundles (for example, installers must not reverse the order of the options buttons across more than one install window).
- Software installers including bundle proxies must not collect or transmit personally identifiable information (PII) without informed user consent.
- Any bundled install packages are considered installers and must abide by the same installation notification, consent, and control guidelines as the main installer.

Deception

Users must have an informed awareness of software that is installed on their system including the functionality of the software and whether it is active. Criteria for determining deceptive behaviors are as follows:

- Information regarding the software publisher, source, website, or other identifying information must be reasonable and accurate.
- The legal conditions of the software installation (for example, software license, EULA) must be clearly indicated in a license agreement.
- Information regarding the software publisher in a Digital Signature must be accurate.
- Software must indicate its behaviors and purpose such that users have a meaningful and accurate understanding of the nature of the technology.
- Software that tracks users' activities, including browsing habits, must not hide, cloak, or mislead the user as to this functionality.
- Software must not disguise its presence or masquerade as another technology (for example, deceptive icons, deceptive Version Information, deceptive .lnk files, etc.).

- Advertisements leading to software downloads must not masquerade as another technology (for example, banner ads with fake close buttons).
- Software must not attempt to hide its presence or the presence of other components or software.
- Software must not obfuscate files, filenames, filepaths, registry entries, and the like, beyond reasonable DRM protection.
- Software must not impair the user's ability to uninstall or remove the program.
- Software uninstall features must adequately remove all functional components of an installation.
- Software must not run third-party processes or programs on the system without prior informed user consent.
- Software must not impair the user's ability to control the software while it runs on the system.
- Software must not install, reinstall, or removal itself or other legitimately installed software without informed user consent or interaction.
- Software must not install other software without clear indication of its relationship to the primary software installation.
- Software must gain informed user consent prior to making or modifying key system settings, including:
  - Installing web browser plugins.
  - Changing browser default home pages.
  - Changing browser default search provider.
  - Changing desktop settings.
  - Changing icons or system colors.
  - Modifying the system hosts file.
  - Adding startup registry entries.
  - Modifying security settings.
- Software that makes key system setting changes must reverse these changes as part of the software uninstall process.

Privacy

Users expect that software does not collect, transmit, or reveal sensitive, private information including passwords and personally identifiable information without the express permission of the user or effected individuals. Personally Identifiable Information (PII) is defined differently among jurisdictions. Criteria for determining objectionable behaviors impacting privacy are as follows:

- Software must not reveal, collect, use, or transmit passwords, biometrics, or other credentials without informed user consent of all impacted users.
- Software must not collect, use, or transmit personally identifiable information (PII) or other sensitive data without informed user consent. PII includes (but is not limited to):
  - Name
  - Address
  - City
  - State
  - Postal code/Zip code
  - Phone number

  - Date of Birth
  - Social Security/tax ID number
  - Passport number
  - Driver's license number
  - Other government-issued identification number
  - Bank account number or other financial account information (for example, PayPal, Apple Pay, Google Wallet, E*TRADE)
  - Credit card number
  - Email address
- Software must not track user online activities such as web browsing habits, instant messaging chats, or keystrokes without informed user consent.
- Software must not allow user communications to be monitored, redirected, or changed without informed user consent.
- Software must not allow a remote user to access or control the system or send remote commands without informed user consent.
- A user must be able to deactivate software which allows a remote user to access or control the system or send remote commands.
- Software must not install a proxy or redirect network traffic to an online proxy or other system without informed user consent.
- Software must not require additional user information before it can be uninstalled (for example, email address).
- Software that collects, stores, or transmits user data (including browser activity), passwords, personally identifiable information, or other sensitive information must offer an easily accessible and clear privacy policy.
- Software must not bypass or facilitate bypassing of other software licensing by using software decipherers or altering another piece of software in such a way that bypasses licensing restrictions.
- Software must not generate license keys for another piece of unrelated software which can facilitate licensing restrictions to be bypassed.
- Tracking software must provide a runtime notice that the software is active (for example, login message, a system tray icon with controls, or an always-on-top notice window).

Intel Security recognizes the privacy concerns of its users and as such will not inhibit a user's pursuit to augment their privacy through other tools. Although these technologies may certainly be abused, many are utilized by individuals concerned for their own safety in oppressive regions or to combat surveillance. Therefore, legitimate tools that offer the following primary behaviors and **do not** exhibit other behaviors expressed in this criteria will not be blocked by Intel Security products:

- Virtual Private Networking (VPN) or other communication encryption.
- File or disk encryption.
- File or disk wiping.
- Steganography.
- Anti-Forensics.
- Computer Anti-Theft.
- Anonymizing Internet/web browsing traffic.
- Home security/surveillance software.

Security

Users expect that software does not impede their system security settings, data confidentiality, or the integrity, stability, or availability of their system and its resources. Criteria for determining objectionable behaviors impacting security are as follows:

- Software must not attempt to evade security features of the system or installed security products (this does not include reasonable DRM protection such as runtime packers, encryptors, etc.).
- Software must not attempt to disable or bypass security features of the system or installed security products.
- Software must not change settings of the operating system, security software, or other unrelated software without informed consent of the user.
- Software must not exploit software or system vulnerabilities.
- Software that requires elevated privileges to execute or that facilitates another application to run with elevated privileges must prompt the user to enter credentials for the elevated user with informed notification of the need to do so.
- Software must not facilitate a denial of service (that is, DOS or DDOS) against an application, system or network through exploit, flooding with network traffic or by any other means.

Advertising

Unexpected advertisements can be a deception to the user. For the purposes of this document, advertising methods may include software which creates pop-ups, pop-unders, slide-ins, or inserts advertisements into the context of a web page. Criteria for determining objectionable advertising behaviors are as follows:

- Software must not provide pop-up, pop-under, or slide-in advertisements without informed user consent.
- Advertisements must not be false or fraudulent, deceptive, misleading, vulgar, pornographic, or offensive.
- Pop-up advertisements must not impair the user's ability to close them or to control their system or other software.
- The closing of one pop-up window must not spawn one or more additional pop-up window.
- Advertisement content or logos must direct the user to germane, related content as indicated.
- Advertisements must be clearly labeled to indicate the program, technology, or product creating it.
- Software must not replace the advertisements of another legitimate site, company, or technology without user consent.
- Software must not insert advertisements into the content of another application or technology without user consent.

Performance, Stability, and User Experience

Users expect that the installation of a piece of software does not severely impact the performance or usability of their system or other software. Additionally, negative side effects or features of the software may adversely impact the user experience including annoying advertisements, impairment

of system or resource usability, and other drains on the system. Users may expect certain speed impacts for come technologies (for example, security, file sharing products). However, unexpected impairments may cause frustrations or indicate other unexpected problems.

Criteria for determining objectionable impacts to system performance, stability, or the user experience are as follows:

- Software must not negatively impact system performance, reliability, or the user experience beyond a reasonable level necessary to provide the functionality agreed to by the user.
- Software must not place a high drain on system resources that result in noticeably slower computer performance without informed user consent.
- Software must not consume large amounts of bandwidth of an Internet connection beyond what is reasonable for the type of technology (that is, P2P, online gaming applications, etc.) without informed user consent.
- Software must not negatively impact the reliability of the system without informed user consent.
- Software must not corrupt the operating system, material components of the system, or other installed software without informed user consent

Notification

Central to the evaluation of software risk is the notion that users must be notified of the software installation and the risks associated with it. Notification can occur using many methods and may differ from technology to technology.

Notification may address specific risk behaviors in the software and may alert users to the risks or changes the software will make. Notification may also provide identification of the software so that the user can trace its origin. Notification must be provided for all identified risk behaviors. General notification features may include, but are not limited to:

- Easily accessible and identifiable notice on software distribution websites that outline risks associated with the installation.
- Easily accessible privacy policy information on websites or in installers specifying any collection or use of personally identifiable information prior to any application installation or collection or transmission of data to a third party.
- Easily accessible and germane End User License Agreement information provided prior to any application installation or collection or transmission of data to a third party.
- Valid and germane digital signatures of binary files identifying the vendor, distributor, or manufacturer of the software.
- Installation windows that offer users an opportunity to select or deselect unwanted options prior to installation or making system modifications.
- Product information in the Resource (.RSRC) Version Information section of Windows binary executable and DLL files that is valid and germane to the vendor, distributor, or manufacturer of the software.
- For command-line tools, accurate product name, and version information.
- For command-line tools, accurate and complete Help information.
- For graphical user interfaces, germane product identification in main windows, window frames, or “About” window.

- Installation paths that include accurate names germane to the installation.
- Filenames that are not randomized to obfuscate or otherwise mask the technology.
- Files and components that are not obfuscated beyond any reasonable DRM protection.
- Embedded Windows binary icons (that is, embedded in the PE file RSRC section) that accurately represent the technology.
- Files or content that are not padded with data that impairs the user's ability to accurately identify the technology, vendor, distributor, or manufacturer.
- For pop-up windows or advertisements, identification in the window frame that indicates the application generating the pop-up.
- Startup menu items that clearly identify the application.
- Desktop shortcut names that are germane to the installation.
- Desktop shortcut icons that are germane to the installation.
- Windows registry key entries that are not obfuscated in a manner that hides the identity of the technology beyond reasonable DRM measures.
- For tracking (for example, keylogger or spyware) software that monitors user online activities, notification that the software is running or active, and is easily visible to all affected users prior to any data or activity collection (for example, login notice, runtime system tray icon, pop-up alert, or warning before any monitoring takes place, etc.).
- For bundled applications, notification of bundled components prior to their installation.
- For software updates, clear indication that the software or components are being updated or that an update is available.
- For Uninstall entries in the system Add/Remove Programs interface, clear identification for the technology.
- For Uninstall entries in the Startup menu, clear identification for the technology.

Consent

Software must obtain and users must provide informed consent to any risks posed by the software prior to the actions of the software. Consent may be obtained through several acceptable means including:

- Originating websites of software distribution.
- Software license agreements.
- Software or website privacy policies.
- Software installation menus (including license and privacy policy information).
- Runtime alerts or notifications (including consent to uninstall).

Control

Users should be able to control the installation process of an application or installation and have fundamental control over the technology once installed including starting and stopping the application. Additionally, a user should be able to adequately uninstall or remove the application from a system once its use is no longer desired.

A user should be able to see that a program is running on their system. This can include system tray icons, entries in browser add-on management interfaces, task manger entries, etc.

Users must also be aware if a program updates itself or its components. Users must also be in control of their personal information and the use or transmission thereof.

- Software that is configured to automatically load at system startup or user login must provide a clear mechanism to disable, adequately adjust this setting, or totally remove the software.
- Software that is not standalone (that is, command-line tool or standalone program/component) must provide a clear uninstall mechanism. Uninstall options may be found in several locations, including:
  - Add/Remove Programs.
  - Windows Start Menu Uninstall feature.
  - Windows System Tray.
  - Menu items within the software user interface.
- Software that is standalone (that is, command-line tool or single-click app) must be able to be removed through standard file delete functionality.
- Software must inform the user if updates are to be downloaded or installed automatically.
- Software that tracks a user's online activities must be easily deactivated or uninstalled.

Disputing a PUP Detection

Intel Security PUP detection may come into question by a user or by the software vendor manufacturing or distributing the technology. Vendors wishing to dispute a PUP detection against their software should submit a Detection Dispute Form to McAfee Labs found at:

https://secure.mcafee.com/apps/mcafee-labs/dispute-form.aspx

Updates to Policy

Due to rapid and frequent software development and distribution, Intel Security reserves the right to modify detection posture against a software or technology or to update this detection policy without prior notice.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com