



Spyware Classification and Terms

Abstract

Fortinet classifies all Spyware threats received under one of several categories. One can determine the classification of a detected Spyware threat by examining the prefix given to the threat name. This document seeks to explain the definitions Fortinet employs in order to categorize Spyware. This document may also be used as a guide to understand the potential harm of certain Spyware threats.

- [Adware](#) - [BHO](#) - [Dialer](#) - [Downloader](#) - [Games](#) - [Hacker Tool](#) -
- [Hijacker](#) - [Joke](#) - [Keylog](#) - [Miscellaneous](#) - [Network Management](#) -
- [Peer-to-Peer](#) - [Plugin](#) - [RAT](#) - [Spyware](#) - [Toolbar](#) -

- **Adware:**

This form of Spyware will typically display advertising content to the user. This advertising content may take many forms, but is typically in the form of Internet browser pop-up advertisements. Under most circumstances a user is not aware of the Adware component being installed on the local machine. That is, an Adware component may be surreptitiously installed along with a desired piece of software. Perhaps even masked as an upgrade for additional functionality in one's web browsing software. There can be a fine line between "Adware" and "Spyware", as often Adware contains a Spyware component. (See the definition of Spyware below.)

- **Browser Helper Object (BHO):**

Browser Helper Objects are designed to be supplementary applications or plug-ins designed to add additional capabilities to a web browser. However, BHOs can be used for malicious purposes. BHOs can also be used to capture search results, install software without user knowledge, display advertisements, change the default web page, and so forth. An operating BHO can be undetectable to a user during regular browser use.

- **Dialers:**

This form of Spyware can be used to make unwanted calls via a user's modem or Internet connection. As with most forms of Spyware it is typically installed without the user's knowledge, or educated consent. In the event that a Dialer is installed a user may discover unexpected toll charges on their phone bill.

- **Downloader:**
Downloaders are malicious applications that retrieve files from a remote location. Typically the files are for local installation. A Downloader application is under most circumstances stealthily installed without user consent or knowledge. There are also times when a Downloader will be installed during the installation of a desired program. One of the signs that a Downloader is operating on a host is the detection of a spurious connection attempt by a personal firewall. Under many circumstances this connection is initiated by an unrecognized application.
- **Games:**
Games are computer programs that are intended for computer users' pastime. Some game or joke programs may include images of pop-culture icons and other famous persons.
- **Hacker Tool:**
Hacker Tools are typically used for security auditing, and analysis. They do however have an alternative purpose. Such tools are typically used to subvert existing network and host security. Hacker Tools can also be downloaded to crack server password files, or overwhelm network servers. Many corporate environments have policies prohibiting the possession of such software.
- **Hijacker:**
These are applications that manipulate the Web browser or other settings to change the user's favorite or bookmarked sites, start pages, or menu options. Some Hijackers have the ability to manipulate DNS settings to reroute DNS requests to a malicious DNS server.
- **Joke:**
These are applications typically received by e-mail, or during an Internet Relay Chat (IRC) session. The intent of Joke software is to cause the user confusion and/or distress. Jokes will often cause undesired visual effects on the user's display. Some Jokes alter the look of the display by changing color schemes or backgrounds. Others will open a large number of Internet browser windows, or display inappropriate content on the screen. Jokes have been reported that analyze the host system seemingly scanning for viruses. Once finished the Joke may inform the user that a selection of randomly selected files are viruses.

- **Keylog:**
Keyloggers are applications that log input to the computer via the keyboard and/or mouse. Keylogging applications under many circumstances are downloaded and installed purposefully by a malicious user. These applications can be used to capture passwords, record instant messaging conversations, sent e-mail and so forth. The Keylogger may record the information locally for later retrieval, possibly by a RAT. Alternatively, some Keyloggers will transmit data to a third party in a remote location. Typically Keylogger applications are operating in an obscured manner.
- **Miscellaneous:**
These applications or components are uncategorized due to multiple functionalities, or otherwise non-malicious behavior. These applications may also qualify as "Grayware".
- **Network Management:**
These are applications that could be used for malicious purposes. They may function as applications that alter network settings, disrupt network security, or possibly cause other forms of network disruption. These applications could also be used for legitimate purposes or in-house research such as risk management amplitude tests.
- **Peer-to-Peer:**
These are applications that are installed to perform file exchanges. They are often used to illegally swap music, movies, and other files. Some P2Ps are being used as an entry-point for viruses.
- **Plugin:**
These are applications that are aimed to add additional programs or features to an existing application in an attempt to control, record, and send browsing preferences or other information back to an external destination.
- **Remote Access/Administration Tool (RAT):**
Software designed to allow system changes remotely. Typically in the form of an executable or server daemon RATs can be both a helpful tool, or a severe security threat. When a host has a RAT server installed a remote user is able to make system changes, install or un-install software, download, upload and edit files. Some advanced RAT programs will even allow viewing of the current screen, and manipulation of the mouse as well. RATs can be installed purposefully as commercial software, or fraudulently

by authors harboring mal-intent. Commercial RATs can also be compromised.

- Spyware:

Spyware typically refers to the component of an Adware that is responsible for tracking a user's activities. Under most circumstances, the activities the author of the Spyware is interested in, are those performed online. The Spyware component will usually report online activities to a central server, or network. This network can then compile a profile of the user's activities. Targeted advertising can then be displayed based on the user's online habits. Under rare circumstances the Spyware can be particularly malicious in that it can report very detailed activities to a third party. This may include personally identifiable data.

- Toolbar:

Toolbars are applications installed into a user's Internet browser. Under most circumstances Toolbars are not hidden from plain view. Toolbars are often installed to augment the capabilities of a Internet browsing software. Toolbars are offered by many legitimate companies for harmless reasons; often allowing easier or faster access to content. This may take the form of offering such things as a search box, or perhaps buttons allowing access to oft-visited websites. Toolbars can however be used to cause undesired browser behavior. Some Toolbars work with Adware (see description for Adware above.) Still others, like BHOs, may re-direct search results, or send personally identifying data or user browsing habits to a third party.