

united states

global sites

products and services

purchase

support

security response

downloads

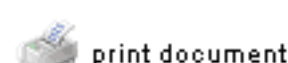
about symantec

search

feedback

Adware.Fapi

Last Updated on: November 13, 2003 12:33:38 PM



Type: [Adware](#)
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows XP
Systems Not Affected: DOS, Linux, Macintosh, OS/2, UNIX
Removal: Low
Damage: Low

detection

- [Intelligent Updater Definitions*](#) October 13, 2003
- [LiveUpdate™ Definitions**](#) October 15, 2003

* Intelligent Updater definitions are released daily, but require manual download and installation. Click [here](#) to download manually.
 ** LiveUpdate definitions are usually released every Wednesday. Click [here](#) for instructions on using LiveUpdate.

This threat can be detected only by Symantec products that support expanded threats. For more information on expanded threats, please go [here](#).

summary

Behavior

Adware.Fapi is an adware component that downloads and displays advertisements.

Symptoms

The files are detected as Adware.Fapi.

Transmission

This adware program is installed with freeware programs, such as "Free History Cleaner" and "Turbo Memory Charger."

technical details

File names: mapisvc32.exe

Adware.Fapi is an adware program that displays advertisements. It is installed with freeware programs, such as "Free History Cleaner" and "Turbo Memory Charger." According to the End-User License Agreement (EULA), the user allows the program to "redirect 404, DNS and other pages" and show "advertisement windows from time to time."

When the software is installed, it performs the following actions to install the adware component:

1. Copies the Mapisvc32.exe file to the %System% folder.

Note: %System% is a variable. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

2. Adds the value:

```
"mapisvc32" = "%System%\mapisvc32.exe"
```

to the registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

removal instructions

The software EULA suggests that the user can remove the adware "service" by uninstalling the software, however we found that this was not the case.

To remove Adware.Fapi, follow these steps:

1. Update the virus definitions.
2. Delete the value that was added to the registry.
3. Run a full system scan and delete all the files detected as Adware.Fapi.

1. Updating the virus definitions

Symantec Security Response fully tests all the virus definitions for quality assurance before they are posted to our servers. There are two ways to obtain the most recent virus definitions:

- Running LiveUpdate, which is the easiest way to obtain virus definitions: These virus definitions are posted to the LiveUpdate servers once each week (usually on Wednesdays), unless there is a major virus outbreak. To determine whether definitions for this threat are available by LiveUpdate, refer to the [Virus Definitions \(LiveUpdate\)](#).
- Downloading the definitions using the Intelligent Updater: The Intelligent Updater virus definitions are posted on U.S. business days (Monday through Friday). You should download the definitions from the Symantec Security Response Web site and manually install them. To determine whether definitions for this threat are available by the Intelligent Updater, refer to the [Virus Definitions \(Intelligent Updater\)](#).

The [Intelligent Updater virus definitions](#) are available: Read "[How to update virus definition files using the Intelligent Updater](#)" for detailed instructions.

2. Deleting the value from the registry

WARNING: Symantec strongly recommends that you back up the registry before making any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify the specified keys only. Read the document, "[How to make a backup of the Windows registry](#)," for instructions.

Note: This is done to make sure all the keys are removed. They may not be there if the uninstaller removed them.

- a. Click Start, and then click Run. (The Run dialog box appears.)
- b. Type `regedit`

Then click OK. (The Registry Editor opens.)

- c. Navigate to the key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

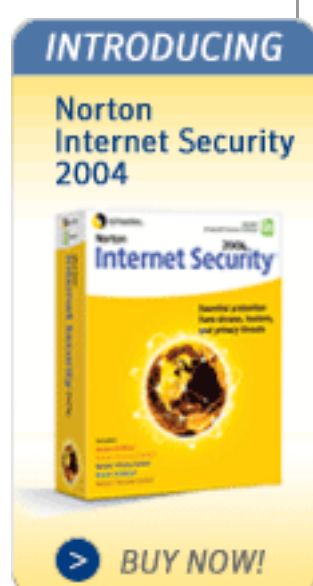
- d. In the right pane, delete the value:

```
"mapisvc32" = "%System%\mapisvc32.exe"
```

- e. Exit the Registry Editor.
- f. Restart the computer.

3. Scanning for and deleting the infected files

- a. Start Norton AntiVirus and make sure that it is configured to scan all the files. For more information, read the document, "[How to configure Norton AntiVirus to scan all files](#)."
- b. Run a full system scan.
- c. If any files are detected as infected with Adware.Fapi, click Delete.



© 1995-2003 Symantec Corporation. All rights reserved.

[Legal Notices](#)

[Privacy Policy](#)