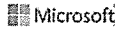


EXHIBIT 17



Account Sign in

Malware Protection Center

Home Security software Malware encyclopedia Our research Help Developers

Follow: TRANSLATE

Win32/Cutwail

Summary

Technical information

Microsoft security software detects and removes this threat.

This threat downloads and runs files on your PC, including a trojan that sends spam emails. It can also steal your email user names and passwords, as well as your FTP credentials, using a plugin detected as PWS:Win32/Fareit.gen!C.

This threat also uses a rootkit and other defensive techniques to avoid detection and removal. Find out ways that malware can get on your PC.

What to do now

The following free Microsoft software detects and removes this threat:

- Windows Defender for Windows 10 and Windows 8.1, or Microsoft Security Essentials for Windows 7 and Windows Vista
- Microsoft Safety Scanner
- Microsoft Windows Malicious Software Removal Tool

You should also run a full scan. A full scan might find other, hidden malware.

Advanced troubleshooting

To restore your PC, you might need to download and run Windows Defender Offline. See our advanced troubleshooting page for more help.

Get more help

You can also ask for help from other PC users at the Microsoft virus and malware community. If you're using Windows XP, see our Windows XP end of support page.

Top

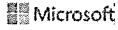
Provide feedback

I want to...

- Get help
- Remove difficult malware
- Avoid tech support phone scams
- See and search the latest threats
- Find answers to other problems
- Fix my software
- Download and update
- Submit a file

Alert level: Severe
This entry was first published on: Nov 29, 2007
This entry was updated on: Sep 15, 2014

This threat is also detected as:
No known aliases



Account Sign in

Malware Protection Center

- Home
- Security software
- Malware encyclopedia
- Our research
- Help
- Developers

Follow:

It then loads the driver. This driver is able to hide processes for a supplied process id (PID) by directly manipulating the EPROCESS structure.

Cutwail usually downloads an updated version of itself. This updated version drops another driver, which implements additional rootkit functionality. The updater tries to write the device driver to:

- `%SystemRoot%\System32\drivers\runtime2.sys`

It installs this driver via the following registry changes:

In subkey: `HKLM\SYSTEM\CurrentControlSet\Services\runtime2\`

Sets value: "ImagePath"

With data: "`\\?\{C:\WINDOWS\System32\drivers\runtime2.sys`"

Sets value: "Type"

With data: "0x1"

Sets value: "ErrorControl"

With data: "0x1"

Sets value: "Start"

With data: "0x3"

It then loads the driver.

If `runtime2.sys` already exists, the new device driver is written to the alternate location:

- `%SystemRoot%\System32\drivers\runtime2.sy_`

The existing device driver is then instructed to update itself with the new copy.

The driver also creates the following registry keys to ensure that is loaded in safe mode:

- `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\runtime2.sys`
- `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\runtime2.sys`

This driver then drops a file to:

- `%TEMP%\startdrv.exe`

It creates the following registry entry to ensure that the dropped file is run:

In subkey: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\`

Sets value: "startdrv"

With data: "`%TEMP%\startdrv.exe`"

Inhibits removal

Cutwail is not only able to hide itself; it can prevent the removal of its files and registry entries. To hide and protect its registry entries, it hooks the following functions via SSDT:

- `ZwDeleteValueKey()`
- `ZwEnumerateKey()`
- `ZwEnumerateValueKey()`
- `ZwOpenKey()`
- `ZwSetValueKey()`

To protect files on disk it implements a file system filter driver. The IRP handlers `IRP_MJ_CREATE` and `IRP_MJ_DIRECTORY_CONTROL` are hooked for the FastFAT or NTFS driver objects, depending on the filesystem type.

Downloads and runs files

Cutwail tries to run Internet Explorer if it exists as this file:

- `%ProgramFiles%\Internet Explorer\iexplore.exe`

It then injects the downloading component into this process, where it runs. Cutwail instructs `runtime.sys` to hide the `iexplore.exe` process. After this, `runtime.sys` is deleted.

The downloading component creates the mutex: `k4j.32H_f7z_Z6e.g8G0`.

It tries to connect to one of the following remote hosts to download a software bundle.

- 66.246.72.173
- 67.18.114.98
- 208.66.194.241
- 66.246.252.213
- 66.246.252.215
- 208.66.194.234

Cutwail creates a file during the download process, selecting the name randomly from the following list:

- `%windir%\system32\9_exception.nls`
- `%windir%\system32\0_exception.nls`
- `%windir%\system32\7_exception.nls`
- `%windir%\system32\6_exception.nls`
- `%windir%\system32\5_exception.nls`
- `%windir%\system32\4_exception.nls`
- `%windir%\system32\3_exception.nls`
- `%windir%\system32\2_exception.nls`
- `%windir%\system32\1_exception.nls`
- `%windir%\system32\0_exception.nls`

Cutwail might also make the following subkey:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Themes\LastTheme\Last`

Executables from within the downloaded software bundle are usually written to disk or injected directly into Internet Explorer. Those which are written to disk are given a random numerical file name and are written to the %TEMP% folder, for example, %TEMP%\1193135.exe.

Analysis by Scott Molenkamp and Shawn Wang

Symptoms

This threat uses advanced stealth (rootkit) functionality to hide its presence. Alerts from your security software may be the only symptom.






Prevention

Take these steps to help prevent infection on your PC.

[Top](#)

[Provide feedback](#)

Other Microsoft sites

-  [Windows](#)
-  [Office](#)
-  [Surface](#)
-  [Windows Phone](#)
-  [Mobile devices](#)
-  [Xbox](#)
-  [Skype](#)
-  [MSN](#)
-  [Bing](#)
-  [Microsoft Store](#)

Downloads

- [Download Center](#)
- [Windows downloads](#)
- [Office downloads](#)

Support

- [Support home](#)
- [Knowledge base](#)
- [Microsoft community](#)











About

- [The MMPC](#)
- [Evaluating our protection](#)
- [MMPC Privacy Statement](#)
- [Microsoft](#)
- [Careers](#)
- [Citizenship](#)
- [Company news](#)
- [Investor relations](#)
- [Site map](#)

Popular resources

- [Security and privacy blogs](#)
- [Security Response Center](#)
- [Security Intelligence Report](#)
- [Microsoft Safety & Security Center](#)
- [Malware Protection Center](#)
- [Security for IT Pros](#)
- [Security for developers](#)
- [Trustworthy Computing](#)

Other Microsoft sites

-  [Windows](#)
-  [Office](#)
-  [Surface](#)
-  [Windows Phone](#)
-  [Mobile devices](#)
-  [Xbox](#)
-  [Skype](#)
-  [MSN](#)
-  [Bing](#)
-  [Microsoft Store](#)

Downloads

- [Download Center](#)
- [Windows downloads](#)
- [Office downloads](#)

Support

- [Support home](#)
- [Knowledge base](#)
- [Microsoft community](#)

About

- [The MMPC](#)
- [Evaluating our protection](#)
- [MMPC Privacy Statement](#)
- [Microsoft](#)
- [Careers](#)
- [Citizenship](#)
- [Company news](#)
- [Investor relations](#)
- [Site map](#)

Popular resources

- [Security and privacy blogs](#)
- [Security Response Center](#)
- [Security Intelligence Report](#)
- [Microsoft Safety & Security Center](#)
- [Malware Protection Center](#)
- [Security for IT Pros](#)
- [Security for developers](#)
- [Trustworthy Computing](#)