

Micr	rosoft					Account * Sign i
Malv	ware Prote	ction Cente	r			ρ
Home	Security software	Malware encyclopedía	Our research	Help	Develope	ers
						Follow: TRANSLATE
Win	32/Cutwail					I want to
V V 11 1.	32) Catwan					Get help
Summary Technical information					n	Remove difficult malware Avoid tech support phone scams See and search the latest threats Find answers to other problems
		and removes this threat. s on your PC, including a	roian that sends sparr	emails. It ca	n also	Fix my software
steal your		asswords, as well as your F				Download and update
This threat also uses a rootkit and other defensive techniques to avoid detection and removal.						covinioad and appraise
Find out w	ays that malware can ge	t on your PC.				Submit a file
What	to do now		•			Alert level: Severe This entry was first published on: Nov 29, 2007 This entry was updated on: Sep 15, 2014
The follow	ing free Microsoft softwa	are detects and removes th	is threat:			This threat is also detected as:
	ws Defender for Windov ndows Vista	vs 10 and Windows 8.1, or	Microsoft Security Ess	entials for W	indows 7	No known aliases
	oft Safety Scanner oft Windows Malicious S	oftware Beneaud Tabl				
		ull scan might find other, h	iddan malwara			
		-	idden maiware.			
Advano	ed troubleshoot	ing				
	your PC, you might need oting page for more hel	l to download and run Wir p.	ndows Defender Offlin	e. See our ac	lvanced	
Get mo	re help					
You can al:	so ask for help from othe	er PC users at the Microsof	t virus and malware co	emmunity.		
If you're us	ing Windows XP, see ou	r Windows XP end of supp	ort page.			•
Тор						
	e se consense e comme su comme e comme e no consense comme de se de comme e medi					
Provide f	eedback					

Micr	osoft						Account → Sign i
Malv	ware Prote	ction Cente	r				۶
Home	Security software	Malware encyclopedia	Our research	Help	Developers		
						Follow:	TRANSLATE
Win	32/Cutwail					I want to	
	Summary		Technical info	ormatior	<u>ר</u>	Remove difficult mal Avoid tech support p See and search the l	phone scams atest threats
Threa	at behavior					Find answers to other	n problems

Installation

Cutwail tries to drop a device driver into your PC, overwriting the original legitimate driver file. The file name differs depending on your operating system, but Cutwail has been known to use one of the following:

- %SystemRoot% \System32\drivers\ip6fw.sys
- %SystemRoot% \System32\drivers\secdrv.sys
- %SystemRoot% \System32\drivers\netdtect.sys

Cutwail then tries to start the corresponding kernel driver by name:

- Ip6Fw
- Secdrv
- NetDetect

This driver tries to restore various system hooks to their original unhooked state. For example, any System Service Descriptor Table (SSDT) hook will be reverted. By doing this, Cutwail is able to circumvent security applications or even other malware which may be installed on your PC.

Payload

Steals passwords

Cutwail contains a plugin that can steal FTP passwords. The plugin is detected as PWS:Win32/Fareit.gen! C. A full list of FTP clients that it can steal passwords from is in the Fareit description.

Cutwail can also steal passwords you have stored in your browser. It steals stored passwords from these

- Internet Explorer
- · Mozilla Firefox
- · Google Chrome

It can also steal user names and passwords from these email clients:

- · Windows Live Mail
- · Microsoft Outlook
- Becky! Internet Mail
- Barca
- IncrediMail
- · The Bat!
- · Mozilla Thunderbird

Provides advanced stealth functionality

Cutwail drops a second device driver to disk:

%SystemRoot% \System32\drivers\runtime.sys

It installs the driver via the following registry changes:

In subkey: HKLM\SYSTEM\CurrentControlSet\Services\runtime\

Sets value: "ImagePath"

With data: "\\??\\C:\\WINDOWS\\System32\\drivers\\runtime.sys"

Sets value: "Type" With data: "0x1"

Sets value: "Start" With data: "0x3"

Alert level: Severe

Submit a file

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

This threat is also detected as:

Download and update

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\

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

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:

- · ZwDeleteValueKev()
- ZwEnumerateKey()
- ZwEnumerateValueKey()
- ZwOpenKey()
- ZwSetValueKev0

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

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
- 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\8_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.

Microsoft community

Prevention

Take these steps to help prevent infection on your PC.

Тор

Provide feedback

Skype

MSN
Bing
Microsoft Store

Other Microsoft sites Downloads About Popular resources Windows Download Center The MMPC Security and privacy blogs Windows downloads Evaluating our protection Office Security Response Center Office downloads MMPC Privacy Statement ☐ Surface Security Intelligence Report Microsoft Windows Phone Careers Microsoft Safety & Security Center Support Citizenship Mobile devices Malware Protection Center Support home 6 Xbox Security for IT Pros Knowledge base

Site map

Microsoft

Contact Us Terms of Use Trademarks Privacy & Cookies About our ads ©2015 Microsoft

Security for developers

Trustworthy Computing

Win32/Cutwail

Other Microsoft sites	Downloads	About	Popular resources
Windows Office	Download Center Windows downloads	The MMPC Evaluating our protection	Security and privacy blogs Security Response Center
□ Surface	Office downloads Support Support home Knowledge base Microsoft community	MMPC Privacy Statement Microsoft Careers	Security Intelligence Report
Windows Phone Mobile devices		Citizenship Company news	Microsoft Safety & Security Center Malware Protection Center
Xbox		Investor relations Site map	Security for IT Pros Security for developers
Skype MSN		·	Trustworthy Computing
Bing -		·	

Contact Us Terms of Use Trademarks Privacy & Cookies About our ads ©2015 Microsoft