Websense® TRITON® ThreatScope™

ThreatScope Analysis Report

For file **fab6adfe5c279146fbc8af74abcfc1f46a338132** uploaded **2012-07-03** at **06:08:23 PM**

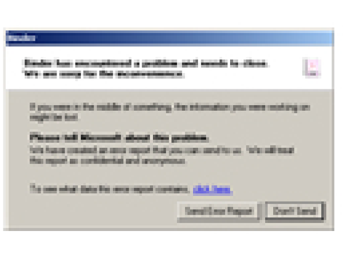
Threat level: **Malicious**

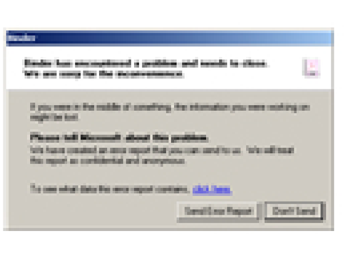
virustotal
View results >

Recommendation: Do not allow this file to be run in your network. Perform remediation on machines on which the file may have run.

Threat	Assessment
!!	Process events show characteristics of a userland rootkit
!!	HTTP traffic shows characteristics of a malware family [ZueS]
!!	Drops and runs executable file(s) in a directory of the user profile often used by malware
!!	Injects and executes code in remote process(es)
!!	HTTP traffic to server hosting malicious content
⚠	Drops executable file(s)
⚠	Writes to the filesystem in a directory of the user profile often used by malware
NA	Executes the Windows command shell program

Screenshots:





File details:

Hash MD5	34101da4902000dcb0143a4e845023b7	File size	233.82 KB
Hash SHA-1	f01bc5e4305ab4e345e12a99259a196766558464	File uploaded	2012-07-03 06:08:23 PM
Hash SHA-256	28680a11e4b3458bac0f88817fcc8509f909d66f0b14eabd0943ca7bb593087e	Report created	2012-07-03 06:10:11 PM

Technical Details

Requested HTTP URLs

The analyzed file requests the following URLs.

URL	IP Address	Category	Details	Method	Status	MIME
www.google.co.kr/webhp	74.125.235.223	Search Engines and Portals		GET	200	text/html; charset=UTF-8
109.169.37.149/~admin/config/gate.php	109.169.37.149	Malicious Web Sites		POST	200	text/html
109.169.37.149/~admin/config/config.bin	109.169.37.149	Malicious Web Sites		GET	200	application/octet-stream
www.google.com/webhp	74.125.235.212	Search Engines and Portals		GET	302	text/html; charset=UTF-8

Resolved hostnames

The analyzed file used DNS to resolve the following hostnames.

Hostname	Category	IP address
www.l.google.com	Search Engines and Portals	74.125.235.212
www.l.google.com	Search Engines and Portals	74.125.235.209
www.l.google.com	Search Engines and Portals	74.125.235.211
www.l.google.com	Search Engines and Portals	74.125.235.208
www.l.google.com	Search Engines and Portals	74.125.235.210
www-cctld.l.google.com	Search Engines and Portals	74.125.235.223
www-cctld.l.google.com	Search Engines and Portals	74.125.235.215
www-cctld.l.google.com	Search Engines and Portals	74.125.235.216

IP addresses

The analyzed file requests the following IP addresses.

IP Address	ASN
74.125.235.223	AS15169 Google Inc.
109.169.37.149	AS20860 Iomart
109.169.37.149	AS20860 Iomart
74.125.235.212	AS15169 Google Inc.

File system modifications

The analyzed file changes the following items in the file system. This type of change can be performed by both malicious and benign files.

Event	File path
Creates file	c:\Documents and Settings\Administrator\Application Data\Vytiub\ocut.exe
Opens file	c:\Documents and Settings\Administrator\Application Data\Vytiub\ocut.exe
Writes file	c:\Documents and Settings\Administrator\Application Data\Vytiub\ocut.exe
Creates file	c:\Documents and Settings\Administrator\Local Settings\Temp\tmp43c431b7.bat
Opens file	c:\Documents and Settings\Administrator\Local Settings\Temp\tmp43c431b7.bat
Writes file	c:\Documents and Settings\Administrator\Local Settings\Temp\tmp43c431b7.bat

Process modifications

The analyzed file affected the following system processes.

Event	File path
Creates process	Sample started
Creates process	C:\WINDOWS\system32\dwwin.exe
Creates process	C:\Documents and Settings\Administrator\Application Data\Vytiub\ocut.exe
Creates process	C:\WINDOWS\system32\cmd.exe
Writes to remote process memory	C:\WINDOWS\explorer.exe
Creates thread in remote process	C:\WINDOWS\explorer.exe
Writes to remote process memory	C:\Program Files\Adobe\Reader 8.0\Reader\reader_sl.exe
Creates thread in remote process	C:\Program Files\Adobe\Reader 8.0\Reader\reader_sl.exe
Writes to remote process memory	C:\WINDOWS\system32\dwwin.exe
Creates thread in remote process	C:\WINDOWS\system32\dwwin.exe
Writes to remote process memory	C:\Documents and Settings\Administrator\Application Data\Vytiub\ocut.exe
Creates thread in remote process	C:\Documents and Settings\Administrator\Application Data\Vytiub\ocut.exe
Writes to remote process memory	C:\WINDOWS\system32\cmd.exe
Creates thread in remote process	C:\WINDOWS\system32\cmd.exe

Registry

No Windows Registry changes were made.

Global system events

The following global system events were detected.

Event	Name
Creates semaphore	C:?WINDOWS?TEMP?34101DA4902000DCB0143A4E845023B7.EXE
Creates event	Global\userenv: User Profile setup event45023b7.exe
Creates semaphore	shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}23b7.exe
Creates event	Global\crypt32LogoffEvent
Creates semaphore	shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}23b7.exe
Creates mutex	Global\{560E8C23-8914-8BDB-890D-617D33D1B1E3}3b7.exe
Creates mutex	SHIMLIB_LOG_MUTEX
Creates semaphore	shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates mutex	ZonesCounterMutex
Creates mutex	ZonesCacheCounterMutex
Creates mutex	ZonesLockedCacheCounterMutex
Creates event	DINPUTWINMM
Creates event	Global\userenv: User Profile setup eventE1}
Creates semaphore	shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore	MsoDWExclusive1280
Creates mutex	c:!documents and settings!administrator!local settings!temporary internet files!content.ie5!
Creates mutex	c:!documents and settings!administrator!cookies!ttings!temporary internet files!content.ie5!
Creates mutex	c:!documents and settings!administrator!local settings!history!history.ie5!iles!content.ie5!
Creates mutex	WininetConnectionMutex
Creates mutex	RasPbFile
Creates event	Local\{C4C4EB67-EE50-1911-890D-617D33D1B1E3}ication Data\Vytiub\ocut.exe
Creates semaphore	C:?DOCUMENTS AND SETTINGS?ADMINISTRATOR?APPLICATION DATA?VYTIUB?OCUT.EXE
Creates event	Global\userenv: User Profile setup eventpplication Data\Vytiub\ocut.exe
Creates semaphore	shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}ication Data\Vytiub\ocut.exe
Creates semaphore	shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}ication Data\Vytiub\ocut.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-C395-FF3879492FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-D794-FF386D482FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-C394-FF3879482FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-1393-FF38A94F2FA6}
Creates semaphore	shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-CF93-FF38754F2FA6}
Creates semaphore	MsoDWExclusive1556
Creates mutex	Global\{F6AF47F6-42C1-2B7A-8B93-FF38314F2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-1392-FF38A94E2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-2B92-FF38914E2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-8792-FF383D4E2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-FB91-FF38414D2FA6}
Creates mutex	Global\{AABBAD76-A841-776E-890D-617D33D1B1E3}
Creates mutex	Global\{AABBAD79-A84E-776E-890D-617D33D1B1E3}
Creates mutex	Global\{CC6F996F-9C58-11BA-890D-617D33D1B1E3}
Creates mutex	Global\{4E17A9FD-ACCA-93C2-890D-617D33D1B1E3}
Creates mutex	Global\{A6577A4D-7F7A-7B82-890D-617D33D1B1E3}
Creates mutex	Global\{A6577A4C-7F7B-7B82-890D-617D33D1B1E3}
Creates mutex	Local\{C7B1CC59-C96E-1A64-890D-617D33D1B1E3}
Creates mutex	Global\{591416AA-139D-84C1-890D-617D33D1B1E3}
Creates mutex	Local\{C7B1CC5A-C96D-1A64-890D-617D33D1B1E3}}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-A791-FF381D4D2FA6}
Creates mutex	Global\{CC6F996F-9C58-11BA-890D-617D33D1B1E3}er_sl.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-6F92-FF38D54E2FA6}er_sl.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-8F92-FF38354E2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-DB91-FF38614D2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-7B91-FF38C14D2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-1B96-FF38A14A2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-5F92-FF38E54E2FA6}
Creates mutex	Global\{CC6F996F-9C58-11BA-890D-617D33D1B1E3}3b7.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-3393-FF38894F2FA6}3b7.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-3794-FF388D482FA6}3b7.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-4B91-FF38F14D2FA6}
Creates mutex	Global\{CC6F996F-9C58-11BA-890D-617D33D1B1E3}cation Data\Vytiub\ocut.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-7791-FF38CD4D2FA6}cation Data\Vytiub\ocut.exe
Creates mutex	Global\{F6AF47F6-42C1-2B7A-6791-FF38DD4D2FA6}
Creates event	Global\SEM32_EVENT_NUPDEXPIAPI_9_C38A14A2FA6}
Creates event	Global\SEM32_EVENT_NUPDEXPIAPI_8_C38A14A2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-6F92-FF38D54E2FA6}
Creates mutex	Global\{F6AF47F6-42C1-2B7A-3794-FF388D482FA6}
Creates event	Global\SEM32_EVENT_NUPDEXPIAPI_8_C38DD4D2FA6}
Creates event	Global\SEM32_EVENT_NUPDEXPIAPI_9_C38DD4D2FA6}

Follow Websense on Facebook, Twitter and Security Labs

websense

websense TRITON