

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 207, Task ID: 828

Task ID:	828
Risk Level:	6
Date Processed:	2016-04-28 13:10:04 (UTC)
Processing Time:	61.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe"
Sample ID:	207
Type:	basic
Owner:	admin
Label:	7ff0657ea1ec0a26569fed2b87f83dd9
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	713112 bytes
MD5:	7ff0657ea1ec0a26569fed2b87f83dd9
SHA256:	45d634e38c42a26976470ef77f6530c6d6e41178bbb926505dec2b6de8190a17
Description:	None

Pattern Matching Results

6 Modifies registry autorun entries

Process/Thread Events

Creates process:	C:\windows\temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe
["C:\windows\temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe"]	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtFMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtFActivated.Default1

File System Events

Opens:	C:\Windows\Prefetch\7FF0657EA1EC0A26569FED2B87F83-10A0A105.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\WINSPOOL.DRV
Opens:	C:\Windows\System32\winpool.drv
Opens:	C:\windows\temp\oledlg.dll
Opens:	C:\Windows\System32\oledlg.dll
Opens:	C:\windows\temp\OLEPRO32.DLL
Opens:	C:\Windows\System32\olepro32.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\Windows\Temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe
Opens:	C:\windows\temp\dwmapl.dll
Opens:	C:\Windows\System32\dwmapl.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\Temp

Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Users\Admin\pdfeditor.dat
Opens:	C:\Windows\Fonts\sserife.fon
Opens:	C:\
Reads from:	C:\Windows\Temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe
Reads from:	C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Creates key:	HKCU\software\pdf editor
Creates key:	HKCU\software\pdf editor\pdfeditor
Creates key:	HKCU\software\pdf editor\pdfeditor\recent file list
Creates key:	HKCU\software\pdf editor\pdfeditor\settings
Creates key:	HKCR\pdfeditor.document
Creates key:	HKCR\pdfeditor.document\defaulticon
Creates key:	HKCR\pdfeditor.document\shell\open\ddeexec
Creates key:	HKCR\pdfeditor.document\shell
Creates key:	HKCR\pdfeditor.document\shell\open
Creates key:	HKCR\pdfeditor.document\shell\print\ddeexec
Creates key:	HKCR\pdfeditor.document\shell\print
Creates key:	HKCR\pdfeditor.document\shell\printto\ddeexec
Creates key:	HKCR\pdfeditor.document\shell\printto
Creates key:	HKCR\pdfeditor.document\shell\open\command
Creates key:	HKCR\pdfeditor.document\shell\print\command
Creates key:	HKCR\pdfeditor.document\shell\printto\command
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\ddl
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop\languageconfiguration
Opens key:	HKCU\control panel\desktop
Opens key:	HKCU\control panel\desktop\muicached
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\system\currentcontrolset\control\error message instrument\
Opens key:	HKLM\system\currentcontrolset\control\error message instrument
Opens key:	HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:	HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:	HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKCU\software\classes\
Opens key:	HKCU\software\classes\clsid
Opens key:	HKCR\clsid
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:	HKCU\software
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\locale
Opens key:	HKLM\system\currentcontrolset\control\nls\locale\alternate sorts

Opens key: HKLM\system\currentcontrolset\control\nls\language groups
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\datastore_v1.0
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback\segoe ui
 Opens key: HKLM\system\currentcontrolset\control\cmf\config
 Opens key: HKCU\software\classes\pdfeditor.document
 Opens key: HKLM\software\classes
 Opens key: HKCU\software\classes\pdfeditor.document\defaulticon
 Opens key: HKCU\software\classes\pdfeditor.document\shell\open\ddeexec
 Opens key: HKCU\software\classes\pdfeditor.document\shell\print\ddeexec
 Opens key: HKCU\software\classes\pdfeditor.document\shell\printto\ddeexec
 Opens key: HKCU\software\classes\pdfeditor.document\shell\open\command
 Opens key: HKCU\software\classes\pdfeditor.document\shell\print\command
 Opens key: HKCU\software\classes\pdfeditor.document\shell\printto\command
 Opens key: HKCU\software\classes\pdf
 Opens key: HKCR\pdf
 Opens key:
 HKLM\software\microsoft\ctf\compatibility\7ff0657ea1ec0a26569fed2b87f83dd9.exe
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\microsoft\ctf\
 Opens key: HKLM\software\microsoft\ctf\knownclasses
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback\ms shell dlg
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback\ms sans serif
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[cwdillegalindllsearch]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKCU\control panel\desktop[preferreduilanguages]
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
 HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[7ff0657ea1ec0a26569fed2b87f83dd9]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\windows[loadappinit_dlls]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
 Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file1]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file2]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file3]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file4]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file5]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file6]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file7]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file8]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file9]
 Queries value: HKCU\software\pdf editor\pdfeditor\recent file list[file10]
 Queries value: HKCU\software\pdf editor\pdfeditor\settings[previewpages]
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]

Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\datastore_v1.0[disable]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\datastore_v1.0[datafilepath]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane1]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane2]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane3]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane4]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane5]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane6]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane7]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane8]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane9]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane10]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane11]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane13]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane14]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane15]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane16]
 Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[safeprocesssearchmode]
 Queries value: HKCR\.pdf[]
 Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
 Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
 Sets/Creates value: HKCR\pdfeditor.document[]
 Sets/Creates value: HKCR\pdfeditor.document\defaulticon[]
 Sets/Creates value: HKCR\pdfeditor.document\shell\open\ddeexec[]
 Sets/Creates value: HKCR\pdfeditor.document\shell\print\ddeexec[]
 Sets/Creates value: HKCR\pdfeditor.document\shell\printto\ddeexec[]
 Sets/Creates value: HKCR\pdfeditor.document\shell\open\command[]
 Sets/Creates value: HKCR\pdfeditor.document\shell\print\command[]
 Sets/Creates value: HKCR\pdfeditor.document\shell\printto\command[]