Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 207, Task ID: 827

Task ID:	827
Risk Level:	6
Date Processed:	2016-04-28 13:10:02 (UTC)
Processing Time:	61.08 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: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EOG
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.AM
Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.AM.IC
Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.AM.IC
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens: C:\WINDOWS\Prefetch\7FF0657EA1EC0A26569FED2B87F83-2D94D2E3.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\winspool.drv
Opens: C:\WINDOWS\system32\oledlg.dll
Opens: C:\WINDOWS\system32\olepro32.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Config
Opens: C:\WINDOWS\system32\shell32.dll

Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\Temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\Temp
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\WINDOWS\Fonts\sserife.fon
Opens: C:\
Reads from: C:\WINDOWS\Temp\7ff0657ea1ec0a26569fed2b87f83dd9.exe

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\software\microsoft\windows nt\currentversion\image file execution options\7ff0657ea1ec0a26569fed2b87f83dd9.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winspool.drv
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oledlg.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\olepro32.dll
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\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKLM\system\setup
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
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\oleaut\userera
Opens key: HKCU\software
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\7ff0657ea1ec0a26569fed2b87f83dd9.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKCU\software\microsoft\plus!\themes\current
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: HKCU\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\langbaraddin\
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
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\ime compatibility[7ff0657ea1ec0a26569fed2b87f83dd9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
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\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\plus!\themes\current[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKCR\.pdf[]
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[]
Value changes:	HKLM\software\microsoft\cryptography\rng[seed]