

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3, Task ID: 11

Task ID:	11
Risk Level:	4
Date Processed:	2016-04-28 12:46:39 (UTC)
Processing Time:	63.48 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe"
Sample ID:	3
Type:	basic
Owner:	admin
Label:	70707b1474e1364c222b5738e7a5ebca
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	316928 bytes
MD5:	70707b1474e1364c222b5738e7a5ebca
SHA256:	f8e4da55708ab83851edcf19c766a83277939d0f486a1be82352f4da69ab61aa
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe
["C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe"]	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfdMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfdActivated.Default1

File System Events

Opens:	C:\Windows\Prefetch\70707B1474E1364C222B5738E7A5E-4D2A5E01.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\mfc100.dll
Opens:	C:\Windows\System32\mfc100.dll
Opens:	C:\windows\temp\MSVCR100.dll
Opens:	C:\Windows\System32\msvcr100.dll
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.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\MSIMG32.dll
Opens:	C:\Windows\System32\msimg32.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\windows\temp\UxTheme.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\Fonts\arial.ttf
Opens:	C:\Windows\system32\mfc100.dll.2.Manifest
Opens:	C:\Windows\system32\mfc100.dll.3.Manifest
Opens:	C:\Windows\system32\mfc100.dll.Manifest

Opens:	C:\windows\temp\MFC100ENU.DLL
Opens:	C:\Windows\System32\mfc100enu.dll
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe.2.Manifest
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe.3.Manifest
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe.Config
Opens:	C:\Windows\Temp\70707b1474e1364c222b5738e7a5ebca.exe
Opens:	C:\Windows\Fonts\sserife.fon
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\system32\UxTheme.dll.Config
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2	
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll	
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\System32\ole32.dll
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Reads from:	C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
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:	HKCU\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key:	HKCU\software\microsoft\windows\currentversion\policies\network
Opens key:	HKCU\software\microsoft\windows\currentversion\policies\cmdlg32
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\system\currentcontrolset\control\cmf\config
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key:	HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
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\software\microsoft\ctf\compatibility\70707b1474e1364c222b5738e7a5ebca.exe
Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
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\windows
nt\currentversion\languagepack\surrogatefallback\ms sans serif
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
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[70707b1474e1364c222b5738e7a5ebca]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
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\customlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe ui]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms sans serif]
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\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
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]