

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 247, Task ID: 988

Task ID:	988
Risk Level:	5
Date Processed:	2016-04-28 13:14:36 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\28dfe62494dde9ffffaa5699b6bbc526.exe"
Sample ID:	247
Type:	basic
Owner:	admin
Label:	28dfe62494dde9ffffaa5699b6bbc526
Date Added:	2016-04-28 12:45:15 (UTC)
File Type:	PE32:win32:gui
File Size:	481280 bytes
MD5:	28dfe62494dde9ffffaa5699b6bbc526
SHA256:	42f56732be91f76f24e446079358e2bec7520c555cde68594311d10bb49dd886
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
5	Packer: UPX
4	Checks whether debugger is present
5	PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\28dfe62494dde9ffffaa5699b6bbc526.exe
["C:\windows\temp\28dfe62494dde9ffffaa5699b6bbc526.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\28DFE62494DDE9FFFFAA5699B6BBC-51A5AA0B.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\28dfe62494dde9ffffaa5699b6bbc526.exe.Local\
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\temp\msimg32.dll
Opens:	C:\Windows\System32\msimg32.dll
Opens:	C:\windows\temp\version.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\winpool.drv
Opens:	C:\Windows\System32\winpool.drv

Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\Temp
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.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\App\Locale\locale
Opens:	C:\Windows\winsxs\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9	
Opens:	C:\Windows\winsxs\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui	
Opens:	C:\windows\temp\DUser.dll
Opens:	C:\Windows\System32\duser.dll
Opens:	C:\Windows\System32\xmlite.dll
Opens:	C:\Windows\System32\en-US\duser.dll.mui
Reads from:	C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

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\dl1
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\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
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\ole
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKCU\software\embarcadero\locales
Opens key:	HKLM\software\embarcadero\locales
Opens key:	HKCU\software\codegear\locales
Opens key:	HKLM\software\codegear\locales
Opens key:	HKCU\software\borland\locales
Opens key:	HKCU\software\borland\delphi\locales
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKLM\software\microsoft\windows\windows error reporting\wmr
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\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\system\currentcontrolset\control\cmf\config
 Opens key: HKLM\system\currentcontrolset\control\keyboard layouts\04090409
 Opens key: HKLM\software\microsoft\directui
 Opens key: HKLM\software\microsoft\ctf\compatibility\28dfe62494dde9ffffaa5699b6bbc526.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\currentversion\policies\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
 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[28dfe62494dde9ffffaa5699b6bbc526]
 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\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
 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\fontsubstitutes[ms
 shell dlg 2]
 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\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]