

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 102, Task ID: 409

Task ID:	409
Risk Level:	4
Date Processed:	2016-04-28 12:58:11 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\003ae6685c54732c3a84f832c6124c28.exe"
Sample ID:	102
Type:	basic
Owner:	admin
Label:	003ae6685c54732c3a84f832c6124c28
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	62032 bytes
MD5:	003ae6685c54732c3a84f832c6124c28
SHA256:	a8c75df7f516907e7a98378dc4accf993ac6e3a548bbbf1faa0cde87148b8de4
Description:	None

Pattern Matching Results

4	Register or unregister a DLL from command line
4	Terminates process under Windows subfolder
4	Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\003ae6685c54732c3a84f832c6124c28.exe
["C:\windows\temp\003ae6685c54732c3a84f832c6124c28.exe"]	
Creates process:	C:\Windows\SysWOW64\regsvr32.exe [C:\Windows\system32\regsvr32 /s /u .\bin\InstallerDlg.dll]
Terminates process:	C:\Windows\SysWOW64\regsvr32.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtftMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtftActivated.Default1

File System Events

Opens:	C:\Windows\Prefetch\003AE6685C54732C3A84F832C6124-0C5C0CD5.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\AppPatch\sysmain.sdb
Opens:	C:\Windows\Temp\003ae6685c54732c3a84f832c6124c28.exe
Opens:	C:\Windows\AppPatch\AcGenral.dll
Opens:	C:\windows\temp\UxTheme.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\windows\temp\WINMM.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\windows\temp\samcli.dll
Opens:	C:\Windows\SysWOW64\samcli.dll

Opens:	C:\windows\temp\MSACM32.dll
Opens:	C:\Windows\SysWOW64\msacm32.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\windows\temp\sfc.dll
Opens:	C:\Windows\SysWOW64\sfc.dll
Opens:	C:\windows\temp\sfc_os.DLL
Opens:	C:\Windows\SysWOW64\sfc_os.dll
Opens:	C:\windows\temp\USERENV.dll
Opens:	C:\Windows\SysWOW64\userenv.dll
Opens:	C:\windows\temp\profapi.dll
Opens:	C:\Windows\SysWOW64\profapi.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\windows\temp\MPR.dll
Opens:	C:\Windows\SysWOW64\mpr.dll
Opens:	C:\windows\temp\003ae6685c54732c3a84f832c6124c28.exe.Manifest
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens:	C:\Windows\SysWOW64\regsvr32
Opens:	C:\Windows\SysWOW64\regsvr32.exe
Opens:	C:\
Opens:	C:\Windows\SysWOW64\ui\SwDRM.dll
Opens:	C:\Windows\Prefetch\REGSVR32.EXE-D5170E12.pf
Opens:	C:\Windows\SysWOW64\regsvr32.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\SysWOW64\regsvr32.exe.Config
Opens:	C:\Windows\SysWOW64\en-US\regsvr32.exe.mui
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\SysWOW64\rpcss.dll
Opens:	C:\Windows\SysWOW64\bin\bin\InstallerDlg.dll
Opens:	C:\Windows\SysWOW64\bin\InstallerDlg.dll
Opens:	C:\Windows\system\bin\InstallerDlg.dll
Opens:	C:\Windows\bin\InstallerDlg.dll
Opens:	C:\Windows\SysWOW64\Wbem\bin\InstallerDlg.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\bin\InstallerDlg.dll
Opens:	C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Reads from:	C:\Windows\SysWOW64\regsvr32.exe
Reads from:	C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\language
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key:	HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
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\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	HKLM\system\currentcontrolset\control\locale\sorting\versions
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows nt\windows file
protection	
Opens key:	HKLM\software\policies\microsoft\windows nt\windows file protection
Opens key:	HKLM\
Opens key:	HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics	
Opens key:	HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize	
Opens key:	HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32	
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility	
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\wow6432node\microsoft\ole
Opens key:	HKLM\software\wow6432node\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\wow6432node\microsoft\oleaut
Opens key:	HKLM\system\currentcontrolset\control\cmf\config
Opens key:	HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:	HKLM\system\currentcontrolset\control\locale\extendedlocale
Opens key:	HKLM\system\currentcontrolset\services\crypt32
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings	
Opens key:	
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings	
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings	
Opens key:	HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\regsvr32.exe	
Opens key:	HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key:	HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key:	HKLM\software\policies\microsoft\windows\appcompat
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key:	HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:	HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\regsvr32.exe	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots	
Opens key:	HKCU\software\classes\
Opens key:	HKCU\software\classes\.dll
Opens key:	HKCR\.dll
Opens key:	HKCU\software\classes\dllfile
Opens key:	HKCR\dllfile
Opens key:	HKCU\software\classes\dllfile\autoregister

Opens key: HKCR\dlfile\autoregister
 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\software\wow6432node\microsoft\ctf\compatibility\003ae6685c54732c3a84f832c6124c28.exe
 Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\wow6432node\microsoft\ctf\
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options[disableusermodecallbackfilter]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[cwdillegalindllsearch]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Queries value:
 HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
 us[alternatecodepage]
 Queries value: HKCU\control panel\desktop[preferreduilanguages]
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
 Queries value: HKCU\software\microsoft\windows
 nt\currentversion\appcompatflags[showdebuginfo]
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value: HKLM\software\policies\microsoft\windows nt\windows file
 protection[knowndlllist]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\compatibility32[003ae6685c54732c3a84f832c6124c28]
 Queries value: HKLM\software\wow6432node\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\cmf\config[system]
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
 reporting\wmr[disable]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
 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\services\crypt32[debugheapflags]
 Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings[disableimprovedzonecheck]
 Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
 settings[security_hkml_only]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[safeprocesssearchmode]
 Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{c7a85eba-c2d1-41ec-c656-ca2c9221e354}]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{c7a85eba-c2d1-41ec-c656-ca2c9221e354}]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[regsvr32]
Queries value: HKCR\.dll[]
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\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]