

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 110, Task ID: 438

Task ID:	438
Risk Level:	5
Date Processed:	2016-04-28 12:59:03 (UTC)
Processing Time:	60.53 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\4a777d2bc8502cecf394a701613e5c81.exe"
Sample ID:	110
Type:	basic
Owner:	admin
Label:	4a777d2bc8502cecf394a701613e5c81
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	180224 bytes
MD5:	4a777d2bc8502cecf394a701613e5c81
SHA256:	8f7cf37e25f2852ceb6c95840991b75622de5f15291c8cf20aad513b005b11a6
Description:	None

Pattern Matching Results

5 PE: Contains compressed section

Process/Thread Events

Creates process:	C:\windows\temp\4a777d2bc8502cecf394a701613e5c81.exe
["C:\windows\temp\4a777d2bc8502cecf394a701613e5c81.exe"]	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
----------------	-----------------------------------------

File System Events

Opens:	C:\Windows\Prefetch\4A777D2BC8502CECF394A701613E5-F737168A.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\4a777d2bc8502cecf394a701613e5c81.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\appatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\mfcd42.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens:	C:\Windows\SysWOW64\msvc60.dll
Opens:	C:\Windows\SysWOW64\odbc32.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\en-US\MFC42.dll.mui
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\SysWOW64\uxtheme.dll

Opens: C:\Windows\Fonts\sserife.fon
Opens: C:\Windows\SysWOW64\dwmapl.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Creates key: HKCU\software\softwareok.de
Creates key: HKCU\software\softwareok.de\fontviewok
Creates key: HKCU\software\softwareok.de\fontviewok\recent file list
Creates key: HKCU\software\softwareok.de\fontviewok\settings
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dl
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: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllexoptions
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\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\system\currentcontrolset\control\lsa\lspalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
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\software\wow6432node\microsoft\bidinterface\loader
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKCU\software
Opens key: HKLM\software\policies\microsoft\sqlclient\windows
Opens key: HKLM\software\microsoft\sqlclient\windows
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
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\system\currentcontrolset\control\nls\sorting\ids
 Opens key:
 HKLM\software\wow6432node\microsoft\ctf\compatibility\4a77d2bc8502cecf394a701613e5c81.exe
 Opens key:
 HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
 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\ms sans serif
 Opens key: HKLM\software\wow6432node\microsoft\ctf\
 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: 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: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value: HKCU\software\microsoft\windows
 nt\currentversion\appcompatflags[showdebuginfo]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\dlloptions[usefilter]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\dlloptions[4a77d2bc8502cecf394a701613e5c81.exe]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\compatibility32[4a77d2bc8502cecf394a701613e5c81]
 Queries value: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\windows[loadappinit_dlls]
 Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
 Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
 Queries value: HKLM\software\microsoft\ole[aggressivemtesting]
 Queries value: HKLM\software\wow6432node\microsoft\bidinterface\loader[:ldrmsg]
 Queries value:
 HKLM\software\wow6432node\microsoft\bidinterface\loader[c:\windows\temp\4a77d2bc8502cecf394a701613e5c81.exe:2920]
 Queries value:
 HKLM\software\wow6432node\microsoft\bidinterface\loader[c:\windows\temp\4a77d2bc8502cecf394a701613e5c81.exe]
 Queries value:
 HKLM\software\wow6432node\microsoft\bidinterface\loader[c:\windows\temp*]
 Queries value: HKLM\software\wow6432node\microsoft\bidinterface\loader[:path]
 Queries value: HKLM\system\currentcontrolset\control\wmi\security[f34765f6-a1be-4b9d-
 1400-b8a12921f704]
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
 reporting\wmr[disable]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file1]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file2]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file3]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file4]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file5]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file6]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file7]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file8]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file9]
 Queries value: HKCU\software\softwareok.de\fontviewok\recent file list[file10]
 Queries value: HKCU\software\softwareok.de\fontviewok\settings[previewpages]
 Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]

Queries value: HKCU\software\softwareok.de\fontviewok\settings[lisens]
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\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
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\wow6432node\microsoft\ctf[enableanchorcontext]