Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3307, Task ID: 735

Task ID:	735
Risk Level:	7
Date Processed:	2016-05-18 10:31:45 (UTC)
Processing Time:	62.58 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"
Sample ID:	3307
Type:	basic
Owner:	admin
Label:	6b78f38317a53920e530cc1e36053242
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	407933 bytes
MD5:	6b78f38317a53920e530cc1e36053242
SHA256:	cd43eae17643cd5510d87ca5b49ddb5b45f73b83c169dcd1102b356633943046
Description:	None

Pattern Matching Results

5 PE: Contains compressed section
7 Writes to memory of system processes
6 Packer: PECompact
2 PE: Nonstandard section
4 Reads process memory

Static Events

Anomaly:	PE: Contains one or more non-standard sections
Packer:	PeCompact

Process/Thread Events

Creates process:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe ["C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"]
Creates process:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe [C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe]
Reads from process:	PID:492 C:\Windows\explorer.exe
Reads from process:	PID:604 C:\Windows\SysWOW64\calc.exe
Writes to process:	PID:1376 C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe
Writes to process:	PID:492 C:\Windows\explorer.exe
Terminates process:	C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles
Opens:	C:\Windows\Prefetch\6B78F38317A53920E530CC1E36053-7800A4C9.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-

controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens: C:\Windows\SysWOW64\winmm.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\winmmbase.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\msvcrt.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\advapi32.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens: C:\Windows\Temp
Opens: C:\
Opens: C:\Windows\SysWOW64\shlwapi.dll
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\SysWOW64\iertutil.dll
Opens: C:\Windows\SysWOW64\wininet.dll
Opens: C:\Windows\SysWOW64\nsi.dll
Opens: C:\Windows\SysWOW64\ws2_32.dll
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\profapi.dll
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg
Reads from: C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe
Reads from:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg

Windows Registry Events

Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\whciconstartup
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\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: 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
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions
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\fipsalgorithmpolicy
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\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: HKCU\software\borland\locales
Opens key: HKLM\software\wow6432node\borland\locales
Opens key: HKCU\software\borland\delphi\locales
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\6b78f38317a53920e530cc1e36053242.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 nt\currentversion
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags\custom\6b78f38317a53920e530cc1e36053242.exe
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\6b78f38317a53920e530cc1e36053242.exe
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\>{22d6f312-b0f6-11d0-94ab-0080c74c7e95}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{3af36230-a269-11d1-b5bf-0000f8051515}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba855-cc51-11cf-aafa-00aa00b6015f}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{45ea75a0-a269-11d1-b5bf-0000f8051515}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{4f645220-306d-11d2-995d-00c04f98bbc9}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{5fd399c0-a70a-11d1-9948-00c04f98bbc9}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{630b1da0-b465-11d1-9948-00c04f98bbc9}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{6bf52a52-394a-11d3-b153-00c04f79faa6}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{6fab99d0-bab8-11d1-994a-00c04f98bbc9}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{7790769c-0471-11d2-af11-00c04fa35d02}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{7c028af8-f614-47b3-82da-ba94e41b1089}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4383}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{89b4c1cd-b018-4511-b0a1-5476dbf70820}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{9381d8f2-0288-11d0-9501-00aa00b911a5}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{9f612429-4a00-3d44-88cf-146da2ee1f92}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{c9e9a340-d1f1-11d0-821e-444553540600}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{e92b03ab-b707-11d2-9cbd-0000f87a369e}
Opens key: HKCU\software\microsoft\active setup\installed components\{9d71d88c-c598-4935-c5d1-43aa4db90836}
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\policies\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key: HKLM\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key: HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
Opens key: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
Opens key: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
Opens key: HKLM\software\policies\microsoft\windows\edgeui
Opens key: HKCU\software\policies\microsoft\windows\edgeui
Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
Opens key: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32

Opens key: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key:
HKLM\software\microsoft\windows\currentversion\photopropertyhandler\containerassociations
Opens key: HKCU\software\microsoft\windows\currentversion\action center
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\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[6b78f38317a53920e530cc1e36053242.exe]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[6b78f38317a53920e530cc1e36053242]
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[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-

65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
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]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-

0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\>{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{3af36230-a269-11d1-b5bf-0000f8051515}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba855-cc51-11cf-aafa-00aa00b6015f}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{45ea75a0-a269-11d1-b5bf-0000f8051515}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{4f645220-306d-11d2-995d-00c04f98bbc9}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{5fd399c0-a70a-11d1-9948-00c04f98bbc9}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{630b1da0-b465-11d1-9948-00c04f98bbc9}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{6bf52a52-394a-11d3-b153-00c04f79faa6}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{6fab99d0-bab8-11d1-994a-00c04f98bbc9}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{7790769c-0471-11d2-af11-00c04fa35d02}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{7c028af8-f614-47b3-82da-ba94e41b1089}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4383}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89b4c1cd-b018-4511-b0a1-5476dbf70820}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{9381d8f2-0288-11d0-9501-00aa00b911a5}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed

components\{9f612429-4a00-3d44-88cf-146da2ee1f92}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{c9e9a340-d1f1-11d0-821e-444553540600}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}[stubpath]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{e92b03ab-b707-11d2-9cbd-0000f87a369e}[stubpath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[displayversion]
Queries value: HKCU\control panel\desktop[paintdesktopversion]
Queries value: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32[]
Queries value: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value: HKLM\software\microsoft\windows\currentversion\photopropertyhandler\containerassociations[{57a37caa-367a-4540-916b-f183c5093a4b}]
Queries value: HKCU\software\microsoft\windows\currentversion\action center[renotifycount]