

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 626, Task ID: 2451

Task ID: 2451
Risk Level: 6
Date Processed: 2016-02-22 05:31:51 (UTC)
Processing Time: 6.52 seconds
Virtual Environment: IntelliVM
Execution Arguments:
"c:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe"

Sample ID: 626
Type: basic
Owner: admin
Label: b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5
Date Added: 2016-02-22 05:26:50 (UTC)
File Type: PE32:win32:gui
File Size: 393212 bytes
MD5: ba04839db97a1b934cd9e470795ccf51
SHA256: b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5
Description: None

Pattern Matching Results

- 4 Reads process memory
- 5 Abnormal sleep detected
- 5 Possible injector
- 6 Tries to detect VM environment

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process:
C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe
["C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe"]
Reads from process: PID: 1104 C:\Windows\explorer.exe
Terminates process:
C:\Windows\Temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\276188B23DF42F38
Creates mutex: \Sessions\1\BaseNamedObjects\AE2F39DFEE6EA723

File System Events

Opens: C:\Windows\Prefetch\B3AF5BCCF7891B0251AAA73F063F1-4CD469AF.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\sechost.dll
Opens: C:\windows\temp\version.dll
Opens: C:\Windows\System32\version.dll
Opens: C:\windows\temp\wsock32.dll
Opens: C:\Windows\System32\wsock32.dll
Opens: C:\windows\temp\winmm.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\windows\temp\atl.dll
Opens: C:\Windows\System32\atl.dll
Opens: C:\windows\temp\wtsapi32.dll
Opens: C:\Windows\System32\wtsapi32.dll
Opens: C:\Windows\System32\imm32.dll
Opens:
C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.ENU
Opens:
C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.ENU.DLL
Opens:
C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.EN
Opens:
C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.EN.DLL
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\windows\temp\VBoxHook.dll
Opens: C:\Windows\system32\VBoxHook.dll
Opens: C:\Windows\system\VBoxHook.dll
Opens: C:\Windows\VBoxHook.dll
Opens: C:\Windows\System32\Wbem\VBoxHook.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\VBoxHook.dll
Opens: C:\WINDOWS\system32\drivers\VBoxMouse.sys
Opens: C:\WINDOWS\system32\drivers\vmmouse.sys
Opens: C:\WINDOWS\system32\drivers\vmhgfs.sys

Opens:	C:\WINDOWS\system32\drivers\vpc-s3.sys
Opens:	C:\WINDOWS\system32\drivers\vpcubus.sys
Opens:	C:\Users\Admin\AppData\Roaming
Opens:	C:\Users\Admin\AppData\Local
Opens:	C:\windows\temp\profapi.dll
Opens:	C:\Windows\System32\profapi.dll
Opens:	C:\ProgramData
Opens:	C:\Users\Admin

Windows Registry Events

Creates key:	HKCU\software\microsoft\internet explorer\main\featurecontrol
Creates key:	HKCU\software\microsoft\internet explorer\international
Creates key:	HKCU\software\d0ddaac5a9
Creates key:	HKLM\software\d0ddaac5a9
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\mui\cached\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\mui\cached
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\system\currentcontrolset\control\locale\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:	HKLM\software\microsoft\ole
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\system\currentcontrolset\services\crypt32
Opens key:	HKLM\software\microsoft\windows\currentversion\internet settings
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key:	HKCU\software\borland\locales
Opens key:	HKCU\software\borland\delphi\locales
Opens key:	HKLM\system\currentcontrolset\control\locale\customlocale
Opens key:	HKLM\system\currentcontrolset\control\locale\extendedlocale
Opens key:	HKLM\software\policies\microsoft\sqlclient\windows
Opens key:	HKLM\software\microsoft\sqlclient\windows
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\31f8160b
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\000000019
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011

Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
 Opens key: HKLM\software\microsoft\windows nt\currentversion
 Opens key: HKU\
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key: HKCU\software\
 Opens key: HKLM\system\currentcontrolset\control\computername
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\setup
 Opens key: HKLM\hardware\devicemap\scsi\scsi port 0\scsi bus 0\target id 0\logical
 unit id 0
 Opens key: HKLM\hardware\description\system
 Opens key: HKLM\system\currentcontrolset\services\disk\enum
 Opens key: HKLM\software\oracle\virtualbox guest additions
 Opens key: HKLM\software\vmware, inc.\vmware tools
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\wireshark.exe
 Opens key: HKLM\software\
 Opens key: HKLM\software\d0ddaac5a9\
 Opens key: HKCU\software\d0ddaac5a9\
 Opens key: HKCU\software\microsoft\windows\currentversion\app paths\wireshark.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\wireshark
 Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\wireshark
 Opens key: HKLM\software\wireshark
 Opens key: HKCU\software\wireshark
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\fiddler.exe
 Opens key: HKCU\software\microsoft\windows\currentversion\app paths\fiddler.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\fiddler2.exe
 Opens key: HKCU\software\microsoft\windows\currentversion\app paths\fiddler2.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\fiddler2
 Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\fiddler2
 Opens key: HKLM\software\microsoft\fiddler2
 Opens key: HKCU\software\microsoft\fiddler2
 Opens key: HKCR\software\ieinspectorsoft\httpanalyzeraddon
 Opens key: HKCU\software\classes\software\ieinspectorsoft\httpanalyzeraddon
 Opens key: HKCR\iehttpanalyzer.httpanalyzeraddon
 Opens key: HKCU\software\classes\iehttpanalyzer.httpanalyzeraddon
 Opens key: HKCR\httpanalyzerstd.httpanalyzerstandalone
 Opens key: HKCU\software\classes\httpanalyzerstd.httpanalyzerstandalone
 Opens key: HKCR\charles.amf.document
 Opens key: HKCU\software\classes\charles.amf.document
 Opens key: HKCR\charles.document
 Opens key: HKCU\software\classes\charles.document
 Opens key: HKLM\software\xk72 ltd folder
 Opens key: HKCU\software\xk72 ltd folder
 Opens key: HKLM\software\microsoft\rpc
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key:
 HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
 Opens key:
 HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
 Opens key:

HKLM\software\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\software\microsoft\windows\currentversion\explorer\knownfolderssettings
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002
Opens key: HKLM\software\microsoft\windows\currentversion\run
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[tsuserenables]
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\locale\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[b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
Queries value: HKLM\system\currentcontrolset\control\locale\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\locale\nls\extendedlocale[en-us]
Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:

[illegible]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storeserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storeserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storeserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\software\microsoft\windows nt\currentversion[installdate]
Queries value: HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup\systemsetupinprogress]
Queries value: HKLM\hardware\description\system\systembiosversion]
Queries value: HKLM\hardware\description\system\videobiosversion]
Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]
Queries value: HKLM\software\d0ddaac5a9[66d841bc]
Queries value: HKLM\software\d0ddaac5a9[3a0ee025]
Queries value: HKCU\software\d0ddaac5a9[3a0ee025]
Queries value: HKCU\software\d0ddaac5a9[66d841bc]
Queries value: HKLM\software\d0ddaac5a9[ff93998e]
Queries value: HKCU\software\d0ddaac5a9[ff93998e]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsiname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\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\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsiname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-

9d55-7b8e7f157091}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parsiname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002[profileimagepath]
Queries value: HKLM\software\microsoft\windows\currentversion\run[]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1206]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2300]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1809]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1206]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[2300]
Value changes: HKCU\software\microsoft\windows\currentversion\internet

