Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 243, Task ID: 973

Task ID: 973

Risk Level: 1

Date Processed: 2016-04-28 13:14:18 (UTC)

Processing Time: 61.19 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\d0073adb10258eeb3ef4019d1fa93819.exe"

Sample ID: 243 Type: basic Owner: admin

Label: d0073adb10258eeb3ef4019d1fa93819

Date Added: 2016-04-28 12:45:15 (UTC)

File Type: PE32:win32:gui File Size: 671209 bytes

MD5: d0073adb10258eeb3ef4019d1fa93819

SHA256: 10f611b3590435d58e3c4852cd314a9fdee26023a3c4957e564c8e2bdd84388a

Description: None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\d0073adb10258eeb3ef4019d1fa93819.exe

["C:\windows\temp\d0073adb10258eeb3ef4019d1fa93819.exe"]
Creates process: C:\Users\Admin\AppData\Local\Temp\is-

 $EB5HC.tmp \ d0073 adb 10258 eeb3 ef4019 d1 fa93819.tmp \ ["C:\Users\Admin\AppData\Local\Temp\is-Particles of the control of$

EB5HC.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp"

/SL5="\$50148,426596,54272,C:\windows\temp\d0073adb10258eeb3ef4019d1fa93819.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

Creates event: \KernelObjects\MaximumCommitCondition

File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\is-EB5HC.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\is-

 $EB5HC.tmp \ \ d0073adb10258eeb3ef4019d1fa93819.tmp$

Creates: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp_isetup

Creates: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp_isetup_RegDLL.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp_isetup_setup64.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp_isetup_shfoldr.dll

Creates: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp\gmsx.exe
Opens: C:\Windows\Prefetch\D0073ADB10258EEB3EF4019D1FA93-EE63A557.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

 $\label{lem:c:windows} Opens: C: \verb|windows| temp| d0073adb10258eeb3ef4019d1fa93819.exe.Local| downward temp| d0073adb102586eef401966eef401966eef401966eef401966eef401966eef40196eef401966eef40196eef40196eef40196eef40196eef40196eef40196eef40196eef40196eef40196eef40196eef40196ee$

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\imm32.dll
Opens: C:\Windows\WindowsShell.Manifest

Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui

Opens: C:\windows\temp\netmsg.dll
Opens: C:\Windows\SysWOW64\netmsg.dll

Opens: C:\Windows\SysWOW64\en-US\netmsg.dll.mui

Opens: C:\Windows\Temp\d0073adb10258eeb3ef4019d1fa93819.exe

Opens: C:\Users\Admin\AppData\Local\Temp

Opens: C:\Users\Admin\AppData\Local\Temp\is-EB5HC.tmp
Opens: C:\Windows\Globalization\SortIng\SortDefault.nls

Opens: C:\Windows\SysWOW64\uxtheme.dll

```
C:\windows\temp\dwmapi.dll
 Opens:
                        C:\Windows\SysWOW64\dwmapi.dll
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-
EB5HC.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp
 Opens:
                        C:\Windows\SysWOW64\apphelp.dll
                        C:\Windows\AppPatch\sysmain.sdb
 Opens:
 Opens:
                        C:\
 Opens:
                        C:\Users
 Opens:
                        C:\Users\Admin
 Opens:
                        C:\Users\Admin\AppData
 Opens:
                        C:\Users\Admin\AppData\Local
                        C:\Windows\Prefetch\D0073ADB10258EEB3EF4019D1FA93-4BD251D3.pf
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-EB5HC.tmp\mpr.dll
                        C:\Windows\SysWOW64\mpr.dll
 Opens:
 Opens:
                        C: \verb|\USers\Admin\AppData\Local\Temp\is-EB5HC.tmp\version.dll|
 Opens:
                        C:\Windows\SysWOW64\version.dll
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-
EB5HC.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp.Local\
                        {\tt C:\Users\Admin\AppData\Local\Temp\is-EB5HC.tmp\dwmapi.dll}
 Opens:
 Opens:
                        C:\Windows\Fonts\StaticCache.dat
 Opens:
                        C:\Windows\SysWOW64\en-US\user32.dll.mui
 Opens:
                        C:\Windows\SysWOW64\ole32.dll
 Opens:
                        C:\Windows\SysWOW64\rpcss.dll
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-EB5HC.tmp\netmsg.dll
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp\_isetup\_shfoldr.dll
 Opens:
                        Opens:
                        C:\Windows\SysWOW64\shfolder.dll
                        C:\Windows\SysWOW64\uxtheme.dll.Config
 Opens:
                        C:\Windows\Fonts\sserife.fon
 Opens:
```

Opens: C:\Windows\Fonts\tahoma.ttf Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\imageres.dll

Opens: C:\Windows\SysWOW64\en-US\imageres.dll.mui Opens: C:\Windows\SysWOW64\en-US\shell32.dll.mui Opens: C:\Windows\Fonts\verdanab.ttf Opens: C:\Windows\SysWOW64\shlwapi.dll

Opens: C:\Program Files (x86)\Common Files\microsoft shared\ink\tiptsf.dll

Opens: $C: \verb|\USers\Admin\AppData\Local\Temp\is-EB5HC.tmp\RICHED20.DLL| \\$

Opens: C:\Windows\SysWOW64\riched20.dll

Opens: C:\Windows\win.ini

Writes to: C:\Users\Admin\AppData\Local\Temp\is-

EB5HC.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp

C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp_isetup_RegDLL.tmp Writes to: Writes to: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp_isetup_setup64.tmp Writes to: $\label{local-Temp} $$C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp_isetup_shfoldr.dll $$$

Writes to: C:\Users\Admin\AppData\Local\Temp\is-9CE06.tmp\gmsx.exe Reads from: $C: \verb|\windows\Temp\d0073adb10258eeb3ef4019d1fa93819.exe|$

C:\Users\Admin\AppData\Local\Temp\is-

EB5HC.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp

Reads from: C:\Windows\Fonts\StaticCache.dat

Reads from: C:\Windows\win.ini

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 $HKLM \ system \ current control set \ control \ srp \ gp \ dll$ Opens key: Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers Opens kev: 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 kev: 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: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ assembly storage roots$ Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\diagnostics Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\compatibility32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility Opens key: $HKLM \ \ \, nt\ \ \, in town 6432 node \ \ \, in town on the current version \ \ \, windows$ 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\software\wow6432node\microsoft\windows\windows error reporting\wmr Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\d0073adb10258eeb3ef4019d1fa93819.tmp 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 $\label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\shell folders$ Opens key: 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\d0073adb10258eeb3ef4019d1fa93819.tmp Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder Opens key: HKLM\system\currentcontrolset\control\nls\locale $\label{locale} \verb|HKLM\system\currentcontrolset\control\nls\locale\alternate sorts \\$ Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens key: $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc fontlink\system link} \\$ Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0 HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\segoe ui Opens key: Opens key: $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - b$ Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens key: HKLM\software\wow6432node\microsoft\ctf\ Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: HKLM\software\microsoft\windows\currentversion HKLM\software\microsoft\windows nt\currentversion Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms sans serif Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\tahoma Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ d0073 adb 10258 eeb 3ef 4019 d1 fa 93819. tmp$ HKCU\software\classes\ Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key: 08002b30309d}\shellfolder Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-terminal explorer \setminus$ 3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum

HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key:

HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key:

Opens key: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

a2d8-08002b30309d}\shellfolder

HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-Opens key:

4442-804e-409d6c4515e9}

Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-

409d6c4515e9}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\shell icons

HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\verdana HKLM\software\wow6432node\policies Opens key:

Opens key: HKCU\software\policies

Opens key: HKCU\software

HKLM\software\wow6432node Opens kev:

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \explorer \autocomplete \end{tabular}$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\autocomplete

Opens key:

HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete

Opens key:

Opens key: HKLM\software\microsoft\com3

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\treatas

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062\\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\progid

 $HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid$ Opens key: Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\progid

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprocserver32

HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprochandler

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprochandler

Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas

Opens key:

HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\progid

 $HKCR \ wow 6432 node \ clsid \ \{03c036f1-a186-11d0-824a-00aa005b4383\} \ \ progid$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{03c036f1-a186-11d0-824a-00aa005b4383\}$

HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\progid

HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid Opens key:

HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-Opens key:

00aa005b4383}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprochandler32

Opens key:

00aa005b4383}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprochandler

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprochandler

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}

Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\treatas

Opens key: $HKCR \ wow 6432 node \ clsid \ \{00bb2763-6a77-11d0-a535-00c04fd7d062\} \ treat as \ tre$ Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\progid

Opens key: $HKCR \setminus wow 6432 \\ node \\ clsid \\ \{00bb2763-6a77-11d0-a535-00c04fd7d062\} \\ \setminus progid$ Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\progid

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler

Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client\
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}

Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\treatas

 Opens key:
 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd97}\treatas

b61bb7cdd997}\progid

b61bb7cdd997}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprochandler

Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprochandler

Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions

Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\software\wow6432node\microsoft\rpc

Opens key: HKLM\system\currentcontrol\computername\activecomputername

Opens key: HKLM\system\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqmclient\windows

Opens key: HKLM\software\microsoft\sqmclient\windows

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\fontsubstitutes

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes

Opens key: $\label{eq:hkcu} \mbox{HKCU\software\microsoft\windows nt\currentversion\windows}$

Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\{d8272644-309e-

41e2-a6ed-cd5bec9aa6fe}_is1

Opens key:

 $\label{lem:hamman} HKLM \software \wow 6432 node \microsoft \windows \current version \ninetall \end{dashed} \ \{d8272644-309e-41e2-a6ed-41e2-a6e$

cd5bec9aa6fe}_is1

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

 $options [\verb|disab| leusermodecall backfilter]|$

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:

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\gre_initialize[disablemetafiles]|\\$

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[d0073adb10258eeb3ef4019d1fa93819]

```
HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\windows[loadappinit dlls]
  Queries value:
                                      HKLM\software\microsoft\ole[pageallocatorusesystemheap]
                                      HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:
  Queries value:
                                      HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
                                      HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:
                                      HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:
                                      HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
                                      HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
                                      HKCU\software\microsoft\windows
  Oueries value:
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
                                      HKLM\software\microsoft\windows
  Queries value:
nt \verb|\currentversion| app compatflags[\{6b39d1b2-7883-4648-94bf-bd5109b4ac48\}]|
  Oueries value:
                                      HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
  Queries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
  Queries value:
                                      HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
                                      \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabul
  Oueries value:
options[disablelocaloverride]
  Oueries value:
                                      HKLM\system\currentcontrolset\control\nls\locale[000004091
  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]
  Oueries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Oueries value:
                                      HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|
  Oueries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                      HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
  Oueries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                                      HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane7]|
  Queries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Oueries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Oueries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                                      HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:
                                      HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane12]|
                                      HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
  Oueries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Oueries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                                      HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:
                                      HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0 fb 58b 01c 4a 4 \} \\ language profile \\ 0 x 000 000 000 \\ \{0001 be a 3 - ed 56 - 483 d - a 2e 2 - a ea e 25577436\} [enable]
                                      HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Oueries value:
  Oueries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version [program files dir]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]
  Oueries value:
                                      HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Oueries value:
                                      HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:
                                      HKLM\software\microsoft\windows nt\currentversion[registeredowner]
                                      HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion[registeredorganization]
  Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ \ explorer [no properties my computer]
```

HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]

```
Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[attributes]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[restrictedattributes]
    Queries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
    Queries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
    Oueries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
    Oueries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
    Queries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
                                                              Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                                                              HKCR \verb|\wow6432| node \verb|\clsid| \{20d04fe0-3aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1069-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-10
    Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
    Queries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[nofilefolderjunction]
    Queries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
    Oueries value:
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
    Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}]
    Queries value:
                                                               HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
    Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ autocomplete [autosuggest]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
    Queries value:
                                                              HKLM\software\microsoft\com3[com+enabled]
    Queries value:
                                                               HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
                                                              HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
    Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                                                             HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
    Oueries value:
00c04fd7d062}\inprocserver32[]
    Queries value:
                                                              HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                                              HKLM\software\microsoft\ole[maxsxshashcount]
    Oueries value:
                                                              HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]
    Oueries value:
    Queries value:
                                                              HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[inprocserver32]
                                                              HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
    Oueries value:
00aa005b4383}\inprocserver32[]
                                                              HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
    Oueries value:
00aa005b4383}\inprocserver32[threadingmodel]
                                                              HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
    Oueries value:
    Oueries value:
                                                              HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                                              HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
    Queries value:
00c04fd7d062}\inprocserver32[]
    Queries value:
                                                              HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
```

```
00c04fd7d062}\inprocserver32[threadingmodel]
  Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
  Queries value:
                                     HKCR \ wow 6432 node \ clsid \ \{807c1e6c-1d00-453f-b920-b61bb7cdd997\}[]
  Queries value:
  Queries value:
                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
  Queries value:
b61bb7cdd997}\inprocserver32[]
  Queries value:
                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
  Oueries value:
                                     HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                     HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                     HKLM\svstem\setup[oobeinprogress]
  Oueries value:
  Queries value:
                                     HKLM\system\setup[systemsetupinprogress]
  Queries value:
                                     HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
                                     HKCU\control panel\desktop[smoothscroll]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui1
  Queries value:
                                      HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
                                     HKCU\software\microsoft\windows nt\currentversion\windows[dragdelav]
  Oueries value:
  Queries value:
                                     HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:
                                     HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
  Oueries value:
                                     HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
transparent]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
transparent bold]
  Queries value:
                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
transparent,01
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
  Oueries value:
transparent bold.01
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[helvetica]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
baltic,186]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
ce,238]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial]
cyr,204]
  Queries value:
                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
greek,161]
  Queries value:
                                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ fontsubstitutes\+ [arial limits] and the limits of the limit
tur.1621
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[courier new baltic,186]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[courier new ce,238]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[courier new cyr,204]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\fontsubstitutes[courier new greek,161]
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\fontsubstitutes[courier new tur,162]
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
  Oueries value:
new roman baltic,186]
  Queries value:
                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
new roman ce,238]
  Queries value:
                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
new roman cyr,204]
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
  Queries value:
new roman greek.1611
  Queries value:
                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
new roman tur,162]
  Queries value:
                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
```

HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma

shell dlg 2] Queries value: armenian]

rmn]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[david

transparent]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[miriam

transparent]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[fixed

miriam transparent]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[rod

transparent]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[fangsong_gb2312]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\fontsubstitutes[kaiti_gb2312]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms

shell dlg] Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]|$