Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 132, Task ID: 529

Task ID: 529

Risk Level: 1

Date Processed: 2016-04-28 13:01:23 (UTC)

Processing Time: 61.2 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.exe"

Sample ID: 132 Type: basic Owner: admin

Label: 2a2824f06d8aa50626c0ce6d634603be

Date Added: 2016-04-28 12:45:03 (UTC)

File Type: PE32:win32:gui File Size: 414810 bytes

MD5: 2a2824f06d8aa50626c0ce6d634603be

SHA256: 499fb3cf2e5aa193e470b23a01ccde14d3414904419844fb2c7954ed0b1f45a6

Description: None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.exe

["C:\windows\temp\2a2824f06d8aa50626c0e6d634603be.exe"]
Creates process: C:\Users\Admin\AppData\Local\Temp\is-

 $F7CLB.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp \ ["C:\Users\Admin\AppData\Local\Temp\is-Picks, Admin\AppData\Local\Temp\is-Picks, Admin\AppData\AppDat$

F7CLB.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp"

/SL5="\$500F8,168902,61952,C:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.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-F7CLB.tmp

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

F7CLB.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp_isetup

Creates: C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp_isetup_RegDLL.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp_isetup_setup64.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp_isetup_shfoldr.dll
Opens: C:\Windows\Prefetch\2A2824F06D8AA50626COCE6D63460-9F80FD5E.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dl1
Opens: C:\Windows\System32\wow64win.dl1
Opens: C:\Windows\System32\wow64cpu.dl1
Opens: C:\Windows\system32\wow64log.dl1

Opens: C:\Windows\SysWOW64

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

Opens: C:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.exe.Local\

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\SysWOW64\imm32.dl1
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\2a2824f06d8aa50626c0ce6d634603be.exe

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

Opens: C:\Users\Admin\AppData\Local\Temp\is-F7CLB.tmp
Opens: C:\Windows\Globalization\SortIng\SortDefault.nls

Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\windows\temp\dwmapi.dll

```
C:\Windows\SysWOW64\dwmapi.dll
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-
F7CLB.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp
                        C:\Windows\SysWOW64\apphelp.dll
 Opens:
 Opens:
                        C:\Windows\AppPatch\sysmain.sdb
 Opens:
 Opens:
                        C:\Users
 Opens:
                        C:\Users\Admin
                        C:\Users\Admin\AppData
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local
                        C:\Windows\Prefetch\2A2824F06D8AA50626C0CE6D63460-61A7E9CD.pf
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-F7CLB.tmp\mpr.dll
 Opens:
                        C:\Windows\SysWOW64\mpr.dll
                        Opens:
 Opens:
                        C:\Windows\SysWOW64\version.dll
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-
F7CLB.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp.Local\
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-F7CLB.tmp\dwmapi.dll
 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-F7CLB.tmp\netmsg.dll
 Opens:
                        C: \label{local-temp} Local \end{temp} is -6TDBA.tmp
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp\_isetup\_shfoldr.dll
 Opens:
                        {\tt C:\Users\Admin\AppData\Local\Temp\is-F7CLB.tmp\shfolder.dll}
 Opens:
                        C:\Windows\SysWOW64\shfolder.dll
 Opens:
                        C:\Windows\SysWOW64\uxtheme.dll.Config
 Opens:
                        C:\Windows\Fonts\sserife.fon
 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
                        C:\Windows\SysWOW64\shlwapi.dll
 Opens:
                        C:\Program Files (x86)\Common Files\microsoft shared\ink\tiptsf.dll
 Opens:
 Opens:
                        \label{local-temp-is-F7CLB.tmp-RICHED20.DLL} C: \USers \land Admin \land App Data \land Local \land Temp \land Is-F7CLB.tmp \land RICHED20.DLL \\
 Opens:
                        C:\Windows\SysWOW64\riched20.dll
 Opens:
                        C:\Windows\win.ini
                        C:\Users\Admin\AppData\Local\Temp\is-
 Writes to:
F7CLB.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp
                        Writes to:
 Writes to:
                        C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp\_isetup\_setup64.tmp
 Writes to:
                        C:\Users\Admin\AppData\Local\Temp\is-6TDBA.tmp\_isetup\_shfoldr.dll
 Reads from:
                        C:\Windows\Temp\2a2824f06d8aa50626c0ce6d634603be.exe
 Reads from:
                        C:\Users\Admin\AppData\Local\Temp\is-
F7CLB.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp
 Reads from:
                        C:\Windows\Fonts\StaticCache.dat
                        C:\Windows\win.ini
 Reads from:
Windows Registry Events
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options
                        Opens key:
 Opens key:
                        HKLM\software\microsoft\wow64
 Opens key:
                        HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
 Opens key:
                        HKLM\system\currentcontrolset\control\safeboot\option
 Opens key:
                        HKLM\system\currentcontrolset\control\srp\gp\dll
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                        HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers
 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 kev:
                        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:
                        Opens key:
                        HKCU\software\policies\microsoft\control panel\desktop
 Opens key:
                        HKCU\control panel\desktop\languageconfiguration
 Opens key:
                        HKCU\control panel\desktop
```

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Wow 6432 node \mbox{\current} windows \current \$

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside

HKCU\control panel\desktop\muicached

Opens key:

Opens key:

```
Opens key:
                                    HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:
                                    HKI M\
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows
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 kev:
                                    HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens kev:
                                    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\2a2824f06d8aa50626c0ce6d634603be.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
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:
                                    HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\2a2824f06d8aa50626c0ce6d634603be.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
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\language groups
  Opens kev:
                                    HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
                                    HKLM\software\microsoft\windows
  Opens key:
nt\currentversion\languagepack\datastore_v1.0
  Opens key:
                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback|
  Opens key:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus compatibility \setminus 2a2824f06d8aa50626c0ce6d634603be.tmp
                                    HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
  Opens kev:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                    HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
  Opens key:
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
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion
  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
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
Opens key:
                                    HKCU\software\classes\
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Opens key:
08002b30309d}\shellfolder
                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-the following of the follow
  Opens kev:
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:
a2d8-08002b30309d}\shellfolder
  Opens kev:
                                    HKCU\software\microsoft\windows\currentversion\policies\nonenum
```

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

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

Opens key: HKCR\drive\shellex\folderextensions

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

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

HKLM\software\wow6432node\policies Opens key:

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

Opens key:

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

HKCU\software\microsoft\windows\currentversion\explorer\autocomplete

Opens key:

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

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ \ autocomplete$

Opens key: HKLM\software\microsoft\com3

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

00c04fd7d062}

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

00c04fd7d062}\treatas

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

. 00c04fd7d062}\progid

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

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

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

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

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

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

00c04fd7d062}\inprochandler

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

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: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{03c036f1-a186-11d0-824a-11d0-$

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

Opens key:

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

HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

Opens key: 00aa005b4383}\progid

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

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

00aa005b4383}\inprocserver32

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

00aa005b4383}\inprocserver32

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

00aa005b4383}\inprochandler32

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

00aa005b4383}\inprochandler32

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

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}

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

00c04fd7d062}\treatas

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

00c04fd7d062}\progid

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

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

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:

 $\label{thm:local-bound} HKLM software \wow6432 node \microsoft \windows \current version \explorer \autocomplete \client \Opens key: HKCU \software \classes \wow6432 node \clied \807c1e6c-1d00-453f-b920-4556f-b920-4556f-b920-4556f-b920-4556f-b920-4556f-b920-4556f-b920-4566f-b920-4556f-b920-4566f$

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: $\label{thm:continuous} \begin{tabular}{ll} HKCR\wow6432\node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ Opens key: \\ HKCU\software\classes\wow6432\node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ \begin{tabular}{ll} HKCU\software\classes\wow6432\node\clsid\c$

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\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: ${\tt HKLM\software\microsoft\sqmclient\windows}$

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: HKCU\software\microsoft\windows nt\currentversion\windows

46bd-b44d-5660e337507f}_is1

Opens key:

5660e337507f}_is1

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

 $options [{\it disable} user {\it modecall} back {\it filter}]$

Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value:

$$\label{lem:hammon} \begin{split} & \text{HKLM} software \\ & \text{policies} \\ & \text{Queries value:} \\ & \text{HKLM} \\ & \text{system} \\ & \text{current control set} \\ & \text{control} \\ & \text{loss of tware } \\ & \text{policies} \\ & \text{microsoft} \\ & \text{windows} \\ & \text{safer} \\ & \text{control} \\ & \text{loss of tware } \\ & \text{loss of twar$$

Queries value:

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]$

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

Queries value: HKLM\system\currentcontrol\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[2a2824f06d8aa50626c0ce6d634603be]
Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

```
Oueries value:
                          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Oueries value:
                          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
                          HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
                          HKCU\software\microsoft\windows
 Oueries value:
nt\current version\app compatflags \hbox{$[\{a9f603c2-b224-4a07-b6ea-a2bcc1a51297\}]$}
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
 Queries value:
                          HKCU\software\microsoft\windows
nt \verb|\currentversion| app compatflags[\{6b39d1b2-7883-4648-94bf-bd5109b4ac48\}]|
 Oueries 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}]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
                          HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Oueries value:
                          HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
 Oueries value:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack \verb|surrogatefallback[plane4]| \\
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
                          HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane8]|
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                          HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane14]|
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                          HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 Oueries value:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
 Queries value:
                          HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
 Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
 Oueries value:
HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current version [common files dir]
                          HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Queries value:
 Queries 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]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
 Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ \ explorer \ [no properties recyclebin]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
```

```
Oueries 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]
  Oueries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries 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]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                                     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-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-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[wantsforparsing]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[queryforoverlay]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[queryforinfotip]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
  Oueries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
  Queries value:
                                      HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
  Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
  Oueries 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}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
  Queries value:
00c04fd7d062}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:
                                     HKLM\software\microsoft\ole[maxsxshashcount]
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
  Oueries value:
00aa005b4383}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[]
  Queries value:
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[threadingmodel]
                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
  Oueries value:
                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
  Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[]
                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
  Queries value:
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
 Oueries value:
 Queries value:
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
 Queries value:
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 Queries value:
b61bb7cdd997}\inprocserver32[]
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 Queries value:
b61bb7cdd997}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                         HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
 Oueries value:
Queries value:
                         HKLM\system\setup[oobeinprogress]
 Queries value:
                         HKLM\system\setup[systemsetupinprogress]
                         HKLM\software\microsoft\samclient\windows[ceipenable]
 Oueries value:
 Queries value:
                         HKCU\control panel\desktop[smoothscroll]
 Queries 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]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
 Queries value:
                         HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
 Queries value:
                         HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
                         HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
 Queries value:
 Oueries value:
                         HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
 Queries value:
                         HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
transparent]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
transparent bold]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
transparent,0]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic
transparent bold,0]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[helvetica]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
baltic,186]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
ce,238]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
cyr,204]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial]
greek,161]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
tur, 162]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[courier new baltic,186]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\fontsubstitutes[courier new ce,238]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[courier new cyr,204]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[courier new greek,161]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\fontsubstitutes[courier new tur,162]
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
new roman baltic,186]
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
 Oueries value:
new roman ce,238]
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
 Queries value:
new roman cyr,204]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
new roman greek, 161]
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times
 Queries value:
new roman tur,162]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma
armenian]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[helv]
```

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

rmn]

 $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus fontsubstitutes [david] \\$ Queries value:

transparent]

 $\label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc mirrors} of t\windows nt\current version\sc fontsubstitutes[miriam]{\sc mirrors} } \mbox{\sc mirrors} \mbox{\$ Queries value: transparent]

Queries value: $\label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ fontsubstitutes [fixed to be a constant of the context of the context$

miriam transparent]

 $\label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ fontsubstitutes[rod]$ Queries value:

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: $\label{lem:hklmsoftware} \verb+MKLM\+ software \verb+\microsoft+ windows nt+ current version+ fontsubstitutes \verb+[ms]+ for the software \verb+\microsoft+ windows nt+ current version+ fontsubstitutes \verb+[ms]+ for the software \verb+\microsoft+ windows nt+ current version+ fontsubstitutes \verb+\m$

shell dlg] Queries value:

 $HKLM \verb| software \verb| microsoft \verb| windows \verb| current version \verb| policies \verb| explorer[turnoff spianimations]| \\$