Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 193, Task ID: 770

Task ID: 770

Risk Level: 1

Date Processed: 2016-04-28 13:08:38 (UTC)

Processing Time: 61.36 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\31c63ffc7b815ef05ebc7d62644e32c5.exe"

Sample ID: 193 Type: basic Owner: admin

Label: 31c63ffc7b815ef05ebc7d62644e32c5

Date Added: 2016-04-28 12:45:10 (UTC)

File Type: PE32:win32:gui File Size: 490424 bytes

MD5: 31c63ffc7b815ef05ebc7d62644e32c5

SHA256: da571c1374f5c0061945319060f660b232d6253b54f4a47982655f617018ed76

Description: None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\31c63ffc7b815ef05ebc7d62644e32c5.exe

["C:\windows\temp\31c63ffc7b815ef05ebc7d62644e32c5.exe"]
Creates process: C:\Users\Admin\AppData\Local\Temp\is-

 $STTAD.tmp \ \ 31c63ffc7b815ef05ebc7d62644e32c5.tmp \ ["C:\Users\Admin\AppData\Local\Temp\is-Particles of the control of the$

STTAD.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp"

/SL5="\$601F4,241567,54272,C:\windows\temp\31c63ffc7b815ef05ebc7d62644e32c5.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

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

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

STTAD.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup

Creates: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup_RegDLL.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup_setup64.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup_shfoldr.dll
Opens: C:\Windows\Prefetch\31C63FFC7B815EF05EBC7D62644E3-0A620AC3.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\31c63ffc7b815ef05ebc7d62644e32c5.exe

Opens: C:\Windows\SysWOW64\ntdl1.dl1
Opens: C:\Windows\SysWOW64\kernel32.dl1
Opens: C:\Windows\SysWOW64\KernelBase.dl1
Opens: C:\Windows\apppatch\sysmain.sdb

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

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

 $\label{lem:controls} Opens: C: \windows \winSxS \x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985 \comctl32.dl1$

Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll

Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll

Opens: C:\Windows\SysWOW64\sspicli.dll Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: C:\Windows\SysWOW64\combase.dll C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\SysWOW64\advapi32.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\msctf.dll Opens: Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\WindowsShell.Manifest

```
C:\Windows\SysWOW64\shlwapi.dll
Opens:
                        C:\Windows\SysWOW64\shell32.dll
Opens:
```

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

Opens: C:\Windows\SysWOW64\uxtheme.dll C:\Windows\SysWOW64\dwmapi.dll Opens: Opens: C:\Users\Admin\AppData\Local\Temp\is-

STTAD.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp

Opens:

C:\Users\Admin\AppData\Local\Temp\is-STTAD.tmp Opens:

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

C:\Windows\Prefetch\31C63FFC7B815EF05EBC7D62644E3-E6BF1E4C.pf Opens:

C:\Windows\SysWOW64\mpr.dll Opens: C:\Windows\SysWOW64\version.dll Opens: C:\Windows\SysWOW64\SHCore.dll Opens: Opens: C:\Windows\SysWOW64\comdlg32.dll

Opens: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup_shfoldr.dll Opens: C:\Windows\SysWOW64\shfolder.dll

C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\Windows\SysWOW64\uxtheme.dll.Config Opens: C:\Windows\Fonts\sserife.fon Opens: C:\Windows\Fonts\tahoma.ttf Opens: C:\Windows\Fonts\StaticCache.dat Opens: C:\Windows\SysWOW64\imageres.dll

Opens: C:\Windows\Fonts\verdanab.ttf Opens: C:\Windows\SysWOW64\clbcatq.dll Opens: C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\tiptsf.dll

Writes to: ${\tt C:\Users\Admin\AppData\Local\Temp\is-}$

STTAD.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp

Writes to: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup_RegDLL.tmp Writes to: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup_setup64.tmp Writes to: C:\Users\Admin\AppData\Local\Temp\is-L79GH.tmp_isetup_shfoldr.dll

Reads from: C:\Windows\Temp\31c63ffc7b815ef05ebc7d62644e32c5.exe

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

STTAD.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp

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

Windows Registry Events

Opens key: HKLM\software\microsoft\wow64 Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

Opens key: $\label{lem:hklmsystem} \verb|HKLM\| system \verb|\currentcontrolset\| control \verb|\mui\| uilanguages \verb|\pendingdelete|| \\$

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\

HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: 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

HKCU\control panel\desktop Opens key:

Opens key: HKCU\control panel\desktop\muicached

Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ microsoft \ windows \ corrent \ windows \ wow \ for the side \ wow \ for the side \ windows \ windows \ wow \ for the side \ wow \ for the side \ windows \ windows \ wow \ for the side \ wow \ for the side \ windows \ windows$ Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

 $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} in the constant of the const$ Opens key:

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

HKLM\software\microsoft\windows Opens key: nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

 $\label{lem:hklm} \mbox{ HKLM\software\wow6432} node\mbox{ microsoft\windows nt\currentversion\ime} \\$ Opens key:

compatibility

Opens key: HKLM\

```
Opens key:
                       HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:
                       HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
```

Opens key: HKLM\system\currentcontrolset\control\lsa

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

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

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 ${\tt HKLM\system\currentcontrolset\control\nls\sorting\ids}$ Opens key: Opens key: HKLM\software\policies\microsoft\sqmclient\windows

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

Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\31c63ffc7b815ef05ebc7d62644e32c5.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: $\label{localization} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current\version\app\compatflags\layers} \\$

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\31c63ffc7b815ef05ebc7d62644e32c5.tmp

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

Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder

Opens key:

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: HKIM\software\microsoft\windows nt\currentversion Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key: $\label{locale} \verb|HKLM\system\currentcontrolset\control\nls\locale\alternate sorts | locale\control\c$

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback

HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback\ms sans serif

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

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

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:

HKCU\software\classes\

Opens key:

Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

Opens key:

08002b30309d}\shellfolder

Opens key:

3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key:

a2d8-08002b30309d}\shellfolder

 $\label{thm:local_hammon} \parbox{$HKCU\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkcu$} \parbox{$$ Opens key:

Opens key:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| policies\\| none num between the content of the co$

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

Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\inprocserver32

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

Opens key: HKCR\drive\shellex\folderextensions

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 Opens key: HKLM\software\wow6432node\policies Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

Opens key:

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

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

Opens key:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\autocomplete| autocomplete| auto$

Opens key:

Opens key: HKLM\software\microsoft\com3

Opens key: HKLM\software\microsoft\windowsruntime\clsid

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}

Opens key: HKCR\activatableclasses\clsid

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

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

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

00c04fd7d062}\inprochandler

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}

Opens key: HKCR\activatableclasses\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: HKCU\software\classes\www6432node\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: $\label{thm:constraint} \begin{tabular}{ll} HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas \\ HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas \\ \end{tabular}$

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

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: HKLM\software\microsoft\windowsruntime\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}

Opens key: HKCR\activatableclasses\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} 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: $\begin{tabular}{ll} HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treat as \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treat as \\ HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treat as \\ HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treat as \\ HKCU\software\classes\wow6432node\clsid\cl$

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprocserver32

 $Opens~key: \\ HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2763-6a77-11d0-a535-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a$

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ autocomplete \ client \ wow for the large substitution \ and \ autocomplete \ client \ wow for the large substitution \ and \ autocomplete \ client \ wow for the large substitution \ autocomplete \ autoco$

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}

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

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

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\currentcontrolset\control\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: 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: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\dnseye_is1

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ dnseye_is 1$

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Oueries 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:

 $\label{thm:current} Queries \ value: \\ HKLM\system\currentcontrolset\control\nls\sorting\versions[]$

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

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

options\dllnxoptions[usefilter]

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

options\dllnxoptions[31c63ffc7b815ef05ebc7d62644e32c5.exe]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[31c63ffc7b815ef05ebc7d62644e32c5] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\system\currentcontrol\sa\fipsalgorithmpolicy[enabled]

Queries value: HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]

Queries value: HKLM\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]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

Queries value: HKLM\software\microsoft\windows

 $nt \verb| current version \verb| app compatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]| \\$

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
 Oueries value: HKLM\software\microsoft\windows

```
nt \verb|\currentversion| app compatflags[{35bf919e-0495-48df-8e74-456384e34e74}]| in the compatflags of the c
   Oueries value:
                                                 HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
                                                 HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
   Queries value:
                                                 HKCU\software\microsoft\windows
nt\current version\app compatflags \hbox{$[$6b39d1b2-7883-4648-94bf-bd5109b4ac48$]}\\
                                                 {\tt HKLM \ } system \verb| current control \verb| session manager[safedll sear chmode] \\
   Queries value:
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[31c63ffc7b815ef05ebc7d62644e32c5.tmp]
                                                 HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
   Oueries value:
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]
                                                 HKLM\software\microsoft\windows\currentversion[programfilesdir]
   Oueries value:
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion[commonfilesdir]
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion[registeredowner]
   Oueries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion[registeredorganization]
                                                 HKLM\svstem\currentcontrolset\control\nls\locale[00000409]
   Oueries value:
   Queries value:
                                                 HKLM\system\currentcontrolset\control\nls\language groups[1]
                                                 HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
   Oueries value:
                                                 HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\datastore\_v1.0[datafilepath]|
                                                 HKLM\software\microsoft\windows
   Queries value:
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]
                                                 HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
                                                 HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                                                 HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane6]|
                                                 HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\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
\verb|nt\currentversion\language| pack\surrogatefallback[plane10]|
                                                 HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|
                                                 HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
   Queries 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]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[attributes]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[foldervalueflags]
   Queries 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}1
```

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\inprocserver32[] HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Queries value: 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] HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab] Queries value: HKLM\software\microsoft\com3[com+enabled] HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[] Oueries value: Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[inprocserver32] HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Oueries value: 00c04fd7d062}\inprocserver32[] HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Oueries value: 00c04fd7d062}\inprocserver32[threadingmodel] HKLM\software\microsoft\ole[maxsxshashcount] Queries value: $HKCR \setminus \{03c036f1-a186-11d0-824a-00aa005b4383\}[]$ Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-Oueries value: 00aa005b4383}\inprocserver32[inprocserver32] HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-Queries value: 00aa005b4383}\inprocserver32[1 Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[threadingmodel] Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[] 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-Oueries value: 00c04fd7d062}\inprocserver32[threadingmodel] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ autocomplete \ \ \ []$ Oueries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[] Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprocserver32[inprocserver32] HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Oueries value: b61bb7cdd997}\inprocserver32[] HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Oueries value: b61bb7cdd997}\inprocserver32[threadingmodel] Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll] Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] HKLM\system\setup[oobeinprogress] Queries value: Oueries value: HKLM\system\setup[systemsetupinprogress] Queries value: HKLM\software\microsoft\rpc[idletimerwindow] Queries value: HKCU\control panel\desktop[smoothscroll] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]

HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]

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

ui]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [turn off spianimations]$