Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 193, Task ID: 773

Task ID: 773

Risk Level: 1

Date Processed: 2016-04-28 13:08:44 (UTC)

Processing Time: 62.51 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-

 $BA762.tmp \ \ 31c63ffc7b815ef05ebc7d62644e32c5.tmp \ \ ["C:\Users\Admin\AppData\Local\Temp\is-Particles of the control of th$

BA762.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp"

/SL5="\$40148,241567,54272,C:\windows\temp\31c63ffc7b815ef05ebc7d62644e32c5.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-BA762.tmp

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

 $BA762.tmp \ \ 31c63ffc7b815ef05ebc7d62644e32c5.tmp$

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

Creates: C:\Users\Admin\AppData\Local\Temp\is-6BFKS.tmp_isetup_RegDLL.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-6BFKS.tmp_isetup_setup64.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-6BFKS.tmp_isetup_shfoldr.dll
Opens: C:\Windows\Prefetch\31C63FFC7B815EF05EBC7D62644E3-0A620AC3.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\31c63ffc7b815ef05ebc7d62644e32c5.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\31c63ffc7b815ef05ebc7d62644e32c5.exe

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

Opens: C:\Users\Admin\AppData\Local\Temp\is-BA762.tmp
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

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

BA762.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp

Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\AppPatch\sysmain.sdb

Opens: C:\Users
Opens: C:\Users\Opens:
Opens: C:\Users\Admin
Opens: C:\Users\Admin

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

Opens: C:\Windows\Prefetch\31C63FFC7B815EF05EBC7D62644E3-D8DB55B6.pf

Opens: C:\Users\Admin\AppData\Local\Temp\is-BA762.tmp\mpr.dll

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

Opens: C:\Users\Admin\AppData\Local\Temp\is-BA762.tmp\version.dll

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

BA762.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp.Local\

Opens: C:\Users\Admin\AppData\Local\Temp\is-BA762.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-BA762.tmp\netmsg.dll

Opens: C:\Users\Admin\AppData\Local\Temp\is-6BFKS.tmp

 $\label{lem:continuous} Opens: $$C:\Users\admin\appData\Local\Temp\is-6BFKS.tmp_isetup_shfoldr.dll$$$

Opens: C:\Users\Admin\AppData\Local\Temp\is-BA762.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
Opens: C:\Windows\SysWOW64\shlwapi.dll

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

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

BA762.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp

 $\label{lem:condition} Reads from: $$C:\Windows\Temp\31c63ffc7b815ef05ebc7d62644e32c5.exe$$

Reads from: C:\Users\Admin\AppData\Local\Temp\is-BA762.tmp\31c63ffc7b815ef05ebc7d62644e32c5.tmp

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

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
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\currentcontrol\sct\control\nls\customlocale
Opens key: HKLM\system\currentcontrol\set\control\nls\language
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages\en-us

 $Opens~key: \\ HKLM\system\current control set\control\mui\uilanguages\pending delete$

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:

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\

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

nt\currentversion\diagnostics

```
Opens key:
                                                               HKLM\software\wow6432node\microsoft\windows
\verb|nt\currentversion\gre_initialize| \\
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\ole
                                                              HKLM\software\wow6432node\microsoft\ole\tracing
    Opens key:
    Opens key:
                                                              HKLM\software\microsoft\ole\tracing
    Opens key:
                                                               HKLM\software\wow6432node\microsoft\oleaut
                                                              HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
    Opens kev:
    Opens key:
                                                               HKLM \verb|\system| current controlset| control \verb|\nls| extended locale
                                                              HKLM\system\currentcontrolset\control\cmf\config
    Opens key:
    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:
                                                               HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
    Opens key:
                                                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\31c63ffc7b815ef05ebc7d62644e32c5.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:
                                                               Opens key:
                                                              HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
    Opens key:
                                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\datastore_v1.0|
    Opens key:
                                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\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 31c63 \\ ffc7b815ef05ebc7d62644e32c5.tmp
                                                              HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be18 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be18 \\ node \setminus microsoft \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be18 \\ node \setminus microsoft \setminus micros
    Opens key:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                              HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - be
    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
                                                              HKI M\software\microsoft\windows
    Opens kev:
nt\currentversion\languagepack\surrogatefallback\ms sans serif
                                                              HKLM\software\microsoft\windows
    Opens key:
nt\currentversion\languagepack\surrogatefallback\tahoma
    Opens key:
Opens key:
                                                               HKLM\software\microsoft\windows\currentversion\policies\explorer
                                                              \label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\policies\explorer}} \\
    Opens key:
    Opens key:
HKCU\software\classes\
    Opens key:
                                                               HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{20d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1069-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d04fe0-3aea-1060-a2d8-42d0466-a2d046fe0-3aea-1060-a2d8-42d046fe0-3aea-1060-a2d8-42d046fe0-3
    Opens key:
08002b30309d}\shellfolder
                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Opens key:
08002b30309d}\shellfolder
                                                              Opens key:
3aea-1069-a2d8-08002b30309d}\shellfolder
    Opens key:
a2d8-08002b30309d}\shellfolder
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\policies\nonenum
    Opens key:
Opens key:
                                                              HKLM\software\microsoft\windows\currentversion\policies\nonenum
                                                              HKCU\software\classes\drive\shellex\folderextensions
    Opens key:
    Opens key:
                                                              HKCR\drive\shellex\folderextensions
    Opens key:
                                                              HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
    Opens key:
                                                               HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
```

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

Opens key:

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

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

HKCU\software Opens key:

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

Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete

HKLM\software\microsoft\com3 Opens key:

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

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} Opens key:

00c04fd7d062}\progid

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

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

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprocserver32

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2765-6a77-11d0-a535-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a75-6a75-6a75-6a77-11d0-a55-6a75-6a75-6a75-6a75-6a75-$

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: 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: $\label{lem:hkcrwow6432} HKCR\wow6432 node \clsid\\ \{03c036f1-a186-11d0-824a-00aa005b4383\\ \\ \treatas$ Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\progid

Opens key: $HKCR\wow6432 node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\ \ progid$ HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key:

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

00aa005b4383}\progid

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

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

00aa005b4383}\inprocserver32

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

00aa005b4383}\inprocserver32

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

00aa005b4383}\inprochandler32

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

00aa005b4383}\inprochandler32

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

00aa005b4383}\inprochandler

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

00aa005b4383}\inprochandler

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

00c04fd7d062}

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

00c04fd7d062}\treatas

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

00c04fd7d062}\progid

Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid Opens key: HKCU\software\classes\clsid\{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 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens key: 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 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens key: 00c04fd7d062}\inprochandler Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler Opens kev: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ autocomplete \ client \ wow 6432 node \ microsoft \ windows \ current \ version \ explorer \ autocomplete \ client \ wow 6432 node \ microsoft \ windows \ current \ version \ explorer \ autocomplete \ client \ wow 6432 node \ microsoft \ windows \ current \ version \ explorer \ autocomplete \ client \ wow 6432 node \ microsoft \ windows \ current \ version \ explorer \ autocomplete \ client \ wow 6432 node \ microsoft \ windows \ current \ wow 6432 node \ microsoft \ windows \ node \ microsoft \ wow 6432 node \ microsoft \ windows \ node \ microsoft \ node \ microsoft \ node \ nod$ Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997} HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\treatas HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\progid $HKCR \setminus wow6432 \\ node \\ clsid \\ \{807c1e6c-1d00-453f-b920-b61bb7cdd997\} \\ \setminus progid$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprocserver32 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key: b61bb7cdd997}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key: b61bb7cdd997}\inprochandler HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key: b61bb7cdd997}\inprochandler Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions Opens kev: HKLM\software\microsoft\rpc\extensions Opens key: HKLM\software\wow6432node\microsoft\rpc Opens key: $HKLM \verb|\system| current control \verb|\computername| active computername| active computername|$ 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: HKCU\software\microsoft\windows\currentversion\uninstall\dnseye_is1 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\dnseye_is1 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter] Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback] HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-Queries value: us[alternatecodepage] Queries value: HKCU\control panel\desktop[preferreduilanguages] Oueries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest] HKLM\system\currentcontrolset\control\nls\sorting\versions[] Oueries value: Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[31c63ffc7b815ef05ebc7d62644e32c5] Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit dlls]

Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries 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]

Queries value: HKLM\system\currentcontrolset\config[system]

```
Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
                                    HKCU\software\microsoft\windows\currentversion\explorer\shell
  Queries value:
folders[cache]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
  Oueries value:
                                    HKCU\software\microsoft\windows
nt \verb|\currentversion| app compatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]| in the content of the content 
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
                                    HKCU\software\microsoft\windows
  Oueries value:
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}]
  Oueries 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]
  Oueries 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]
  Oueries value:
                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane1]|
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:
                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                                    HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane12]|
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                                    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\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]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Oueries 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-
  Queries value:
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
  Oueries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
                                     Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                     HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{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-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-1
  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}1
                                     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]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
  Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
                                     HKLM\software\microsoft\com3[com+enabled]
  Queries value:
                                     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-
  Queries value:
00c04fd7d062}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                                     HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]
  Queries value:
  Queries value:
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
  Queries value:
00aa005b4383}\inprocserver32[]
  Queries value:
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[threadingmodel]
                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
  Oueries 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]
  Oueries 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]
  Queries value:
                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[]
```

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]

Queries value: HKCU\control panel\desktop[smoothscroll]

Queries value:

 $\label{thm:local_equation} \begin{tabular}{l} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[enableballoontips]| \\$

Oueries value:

 $\label{thm:cu} \parbox{$HKCU$\software\mbox{$microsoft\windows\currentversion}\explorer\advanced[listviewalphaselect]$} \parbox{$dvanced(listviewalphaselect).}$

Queries value:

 $\label{limit} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| [listviews hadow] \\ \end{tabular}$

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]

Oueries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [used ouble click timer]$

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

ui]

Queries value:

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