Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 243, Task ID: 970

Task ID: 970

Risk Level: 1

Date Processed: 2016-04-28 13:14:16 (UTC)

Processing Time: 61.09 seconds
Virtual Environment: IntelliVM

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

Sample ID: 243
Type: basic
Owner: admin

Label: d0073adb10258eeb3ef4019d1fa93819

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

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

MD5: d0073adb10258eeb3ef4019d1fa93819

SHA256: 10f611b3590435d58e3c4852cd314a9fdee26023a3c4957e564c8e2bdd84388a

Description: None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

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

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

V2465.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp"

/SL5="\$30072,426596,54272,C:\windows\temp\d0073adb10258eeb3ef4019d1fa93819.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\is-V2465.tmp

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

V2465.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup

Creates: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup_RegDLL.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup_setup64.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup_shfoldr.dll

Creates: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp\gmsx.exe

Opens: C:\Windows\Prefetch\D0073ADB10258EEB3EF4019D1FA93-EE63A557.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\d0073adb10258eeb3ef4019d1fa93819.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

Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll

Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\user32.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 C:\Windows\SysWOW64\combase.dll Opens: C:\Windows\SysWOW64\oleaut32.dll Opens: Opens: C:\Windows\SysWOW64\advapi32.dll C:\Windows\SysWOW64\imm32.dll Opens: Opens: C:\Windows\SysWOW64\msctf.dll Opens: C:\Windows\SysWOW64\ole32.dll

```
C:\Windows\WindowsShell.Manifest
Opens:
                       C:\Windows\SysWOW64\shlwapi.dll
Opens:
Opens:
                       C:\Windows\SysWOW64\shell32.dll
Opens:
                       C:\Windows\SysWOW64\netmsg.dll
Opens:
                       C:\Windows\Globalization\SortIng\SortDefault.nls
                       C:\Windows\SysWOW64\uxtheme.dll
Opens:
Opens:
                       C:\Windows\SysWOW64\dwmapi.dll
```

Opens:

V2465.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp Opens: C:\Users\Admin\AppData\Local\Temp\is-V2465.tmp

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

C:\Windows\Prefetch\D0073ADB10258EEB3EF4019D1FA93-5E8BF473.pf Opens:

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

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

Opens: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup_shfoldr.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\Fonts\StaticCache.dat Opens: C:\Windows\SysWOW64\imageres.dll Opens: C:\Windows\Fonts\verdanab.ttf Opens: C:\Windows\SysWOW64\clbcatq.dll

Opens:

Opens: C:\Windows\SysWOW64\riched20.dll Opens: C:\Windows\SysWOW64\usp10.dll Opens: C:\Windows\SysWOW64\msls31.dll

Opens: C:\Windows\win.ini

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

V2465.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp

Writes to: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup_RegDLL.tmp Writes to: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup_setup64.tmp Writes to: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp_isetup_shfoldr.dll

Writes to: C:\Users\Admin\AppData\Local\Temp\is-N6EKD.tmp\gmsx.exe Reads from: C:\Windows\Temp\d0073adb10258eeb3ef4019d1fa93819.exe

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

V2465.tmp\d0073adb10258eeb3ef4019d1fa93819.tmp

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

Reads from: C:\Windows\win.ini

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 $\label{lem:hklm} \verb+Kklm \ system \ current control \verb+ wui \ uilanguages \verb+ pending delete \\$ Opens key:

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

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

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

HKCU\control panel\desktop\muicached Opens kev:

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

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 kev: nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens key:

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

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

execution options

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

```
Opens key:
                                                                                  HKLM\software\wow6432node\microsoft\windows
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:
                                                                                 HKI M\
     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
                                                                                 HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
     Opens key:
                                                                                  HKLM\system\currentcontrolset\control\nls\extendedlocale
     Opens key:
     Opens key:
                                                                                 HKLM\system\currentcontrolset\control\nls\sorting\ids
     Opens key:
                                                                                 HKLM\software\policies\microsoft\sqmclient\windows
     Opens key:
                                                                                  HKLM\software\microsoft\sqmclient\windows
     Opens key:
                                                                                 \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \makebox{} current version \makebox{} \mbox{} direct manipulation
     Opens key:
                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\d0073adb10258eeb3ef4019d1fa93819.tmp
     Opens key:
                                                                                 HKLM\system\currentcontrolset\control\session manager\appcertdlls
     Opens key:
                                                                                 HKLM\system\currentcontrolset\control\session manager\appcompatibility
     Opens key:
                                                                                 HKLM\software\wow6432node\policies\microsoft\windows\appcompat
     Opens key:
                                                                                  HKLM\software\policies\microsoft\windows\appcompat
                                                                                 HKCU\software\microsoft\windows\currentversion\explorer\shell folders
     Opens key:
     Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
     Opens key:
                                                                                  \label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \microsoft \windows nt \current version \approximates \mbox{$1$} approximates \mbo
     Opens key:
                                                                                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\d0073adb10258eeb3ef4019d1fa93819.tmp
                                                                                 \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + approximately against the proposed statement of the proposed stat
     Opens key:
     Opens key:
                                                                                  HKLM\system\currentcontrolset\control\session manager
     Opens kev:
                                                                                 HKLM\system\currentcontrolset\control\networkprovider\hworder
     Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ d0073 adb 10258 eeb 3ef 4019 d1 fa 93819. tmp 1007 adb 1007
     Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\ctf\
     Opens key:
                                                                                  HKLM\software\wow6432node\microsoft\ctf\knownclasses
                                                                                  HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version
     Opens key:
                                                                                 HKLM\software\microsoft\windows\currentversion
     Opens key:
                                                                                 HKLM\software\microsoft\windows nt\currentversion
     Opens key:
     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 key:
                                                                                 HKLM\software\microsoft\windows
\verb|nt\current| version \verb|\language| pack \verb|\datastore\_v1.0|
     Opens key:
                                                                                 HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefall back|
     Opens key:
                                                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms sans serif
                                                                                 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in k \end{tabular} in k \end{tabular} and \end{tabular} in k \end{tabular} in k \end{tabular} and \end{tabular} in k \end{tabu
     Opens key:
     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:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ d0073 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d1073 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 d1 fa 93819, tmp \ d279 adb 10258 eeb 3ef 4019 eeb 3ef 4
                                                                                 HKCU\software\classes\
     Opens key:
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}\shellfolder
                                                                                 Opens key:
 3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens kev:
a2d8-08002b30309d}\shellfolder
                                                                                 HKCU\software\microsoft\windows\currentversion\policies\nonenum
     Opens key:
     Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum
     Opens key:
                                                                                 HKLM\software\microsoft\windows\currentversion\policies\nonenum
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
```

HKCU\software\classes\drive\shellex\folderextensions

HKCR\drive\shellex\folderextensions

Opens key: 4442-804e-409d6c4515e9}

Opens key:

Opens key:

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

409d6c4515e93

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 HKLM\software\wow6432node

Opens key: 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:

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

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}

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

00c04fd7d062}\treatas

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

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler

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

00c04fd7d062}\inprochandler

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

00aa005b43833

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

00aa005b4383} Opens key:

HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{03c036f1-a186-11d0-824a-b140-$ 00aa005b4383}\treatas

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

00aa005b4383}\inprocserver32

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

00aa005b4383}\inprocserver32

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

00aa005b4383}\inprochandler32

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

00aa005b4383}\inprochandler32

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

00aa005b4383}\inprochandler

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

00aa005b4383}\inprochandler

Opens key:

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

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler32

Opens key:

00c04fd7d062}\inprochandler

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

00c04fd7d062}\inprochandler

Opens key:

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

Opens key: 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\www6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}

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

b61bb7cdd997}\treatas

Opens key: $\begin{tabular}{ll} HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treat as \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treat as \\ HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treat as \\ HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treat as \\ HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treat as \\ HKCU\software\clsid\clsi$

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 nt\currentversion\windows

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

41e2-a6ed-cd5bec9aa6fe}_is1

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ \{d8272644-309e-41e2-a6ed-cd5bec9aa6fe\}_{is1}$

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

Queries value: HKLM\system\currentcontrol\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:

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

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[d0073adb10258eeb3ef4019d1fa93819.exe]
Queries value: HKLM\software\microsoft\windows

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

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\system\currentcontrol\set\control\lsa\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]

```
Oueries value:
                         HKLM\software\microsoft\sqmclient\windows[ceipenable]
 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}]
 Queries value:
                         HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
 Oueries value:
                         HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\current version\app compatflags \hbox{$[$6b39d1b2-7883-4648-94bf-bd5109b4ac48$]}$}
                         HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
                         HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value:
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[d0073adb10258eeb3ef4019d1fa93819.tmp]
                         HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
 Oueries value:
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]
                         HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion[commonfilesdir]
 Queries value:
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion[registeredowner]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion[registeredorganization]
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\language groups[1]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\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]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                         HKLM\software\microsoft\windows
 Oueries value:
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]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane15]|
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
 Queries value:
Oueries 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]

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

Oueries value:

```
08002b30309d}\shellfolder[attributes]
                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[restrictedattributes]
  Oueries value:
                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[foldervalueflags]
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}]
  Queries value:
                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
  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]
                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
  Oueries value:
  Queries value:
                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[]
  Queries value:
                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
  Queries value:
                                    HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]
                                    HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
  Oueries value:
00aa005b4383}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
  Queries value:
00aa005b4383}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
  Queries value:
                                    HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[]
  Queries value:
                                    HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
                                    HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
  Oueries value:
                                    HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
  Queries value:
b61bb7cdd997}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
  Queries value:
b61bb7cdd997}\inprocserver32[]
  Oueries value:
                                    HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
                                    HKLM\system\setup[oobeinprogress]
                                    HKLM\system\setup[systemsetupinprogress]
  Queries value:
                                    HKLM\software\microsoft\rpc[idletimerwindow]
  Queries value:
                                    HKCU\control panel\desktop[smoothscroll]
  Oueries value:
  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:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
                                    HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
  Queries value:
ui1
  Oueries 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:
  Queries 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,0]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic

transparent bold,0]

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

transparent bold]

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

transparent]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new cyr,204]

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

new roman cyr,204]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\fontsubstitutes[helvetica]

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

ce,238]

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

shell dlg 2]

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

transparent]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new tur,162]

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

new roman tur,162]

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

transparent]

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

new roman ce,238]

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

greek, 161]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[kaiti_gb2312]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new ce,238]

 $\label{thm:local_queries} Queries \ value: \\ HKLM \ software \ microsoft \ windows \ nt \ current version \ fontsubstitutes \ [arial] \\$

baltic,186]

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

armenian]

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

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

tur.1621

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

rmn]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new greek,161]

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

new roman baltic,186]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial cyr,204]

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

transparent]

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new baltic,186]

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

new roman greek,161]

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

miriam transparent]

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

shell dlg]
Oueries value:

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