# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 132, Task ID: 526

Task ID: 526

Risk Level: 1

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

Processing Time: 61.05 seconds
Virtual Environment: IntelliVM

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

Sample ID: 132 Type: basic Owner: admin

Label: 2a2824f06d8aa50626c0ce6d634603be

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

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

MD5: 2a2824f06d8aa50626c0ce6d634603be

SHA256: 499fb3cf2e5aa193e470b23a01ccde14d3414904419844fb2c7954ed0b1f45a6

Description: None

# Pattern Matching Results

### Static Events

Anomaly: PE: Contains a virtual section

#### Process/Thread Events

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

["C:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.exe" ]
Creates process: C:\Users\Admin\AppData\Local\Temp\is-

 $\label{thm:local} QVB01.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp ["C:\Users\Admin\AppData\Local\Temp\is-Particles of the property of the pro$ 

QVB01.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp"

/SL5="\$5006E,168902,61952,C:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.exe" ]

#### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

## File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\is-QVB01.tmp

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

QVB01.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp\\_isetup

Creates: C:\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp\\_isetup\\_RegDLL.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp\\_isetup\\_setup64.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp\\_isetup\\_shfoldr.dll
Opens: C:\Windows\Prefetch\2A2824F06D8AA50626COCE6D63460-9F80FD5E.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\2a2824f06d8aa50626c0ce6d634603be.exe

Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb

Opens: C:\Windows\WinSxS\x86\_microsoft.windows.common-

controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985

 $Opens: C: \windows \winSxS \x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985 \comctl32.dl1$ 

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\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
                         C:\Windows\SysWOW64\dwmapi.dll
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\is-
QVB01.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp
 Opens:
```

C:\Users\Admin\AppData\Local\Temp\is-QVB01.tmp

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\2A2824F06D8AA50626C0CE6D63460-E0895481.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-7M7B8.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

C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\tiptsf.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

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

QVB01.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp

C:\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp\\_isetup\\_RegDLL.tmp Writes to: Writes to:  $C: \verb|\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp\_isetup\_setup64.tmp|$ Writes to: C:\Users\Admin\AppData\Local\Temp\is-7M7B8.tmp\\_isetup\\_shfoldr.dll

Reads from: C:\Windows\Temp\2a2824f06d8aa50626c0ce6d634603be.exe

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

QVB01.tmp\2a2824f06d8aa50626c0ce6d634603be.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 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings Opens key: HKLM\software\policies\microsoft\mui\settings Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: Opens key:  $\label{lem:hklm} \verb+Kklm \system \current control \ \verb+wui \settings \language configuration \\$ 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 kev: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

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

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

Opens kev:

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

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

execution options

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

options\dllnxoptions

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

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\

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:

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} which is the local control of the local control of$ 

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

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

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

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
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\2a2824f06d8aa50626c0ce6d634603be.tmp

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

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

Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\2a2824f06d8aa50626c0ce6d634603be.tmp

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

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ 2a2824f06d8aa50626c0ce6d634603be.tmp$ 

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

Opens key: HKLM\software\www6432node\microsoft\ctf\knownclasses
Opens key: HKLM\software\www6432node\microsoft\windows\currentversion

Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows nt\currentversion
Opens key: HKLM\system\currentcontrol\nls\locale

Opens key: HKLM\system\currentcontrol\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrol\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

Opens key: HKLM\software\microsoft\windows 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

Opens key:

 $HKLM \label{lem:hklm} LKLM \label{lkklm} HKLM \label{lkklm} Wow 6432 node \label{lkklm} icrosoft \label{lkklm} windows \label{lkklm} current version \label{lkklm} policies \label{lkklm} lem \label{lkklm} LKLM \label{lkklm} AKLM \label{lkklm} Wow 6432 node \label{lkklm} windows \label{lkklm} lkklm \label{lkklm} lkklm \label{lkklm} Wow 6432 node \label{lkklm} windows \label{lkklm} lkklm \label{lkklm} Wow 6432 node \label{lkklm} Wow 6432 node \label{lkklm} windows \label{lkklm} lkklm \label{lkklm} windows \label{lkklm} lkklm \label{lkklm} Wow 6432 node \label{lkklm} Wow 6432 node \label{lkklm} windows \label{lkklm} windows \label{lkklm} Wow 6432 node \label{lkklm} Wow 6432 node \label{lkklm} windows \label{lkklm} Wow 6432 node \label{lkklm} Wow 6432$ 

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 2a2824f06d8aa50626c0ce6d634603be.tmp$ 

Opens key: HKCU\software\classes\

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: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum

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

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

08002b30309d}\inprocserver32

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

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}

Opens key:

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

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

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

Opens key:

HKLM\software\microsoft\com3 Opens kev:

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

Opens key: 

00c04fd7d062}

Opens key: HKCR\activatableclasses\clsid

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

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}\inprocserver32

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

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler

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

00c04fd7d062}\inprochandler

Opens kev: 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\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}

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

00aa005b4383}\treatas

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

00aa005b4383}\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

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:

00c04fd7d062}

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

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

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

00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler

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

00c04fd7d062}\inprochandler

Opens key:

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

Opens key: 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

Opens key:  $\label{thm:continuous} \begin{tabular}{ll} HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ \end{tabular}$ 

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: 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\{f5a6a617-1a5c-

46bd-b44d-5660e337507f}\_is1

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ \{f5a6a617-1a5c-46bd-b44d-5660e337507f\}_{is1}$ 

Queries value:

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

Queries value:

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

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

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value:

 $HKLM \label{lem:hklm} White the latest of the latest of$ 

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[2a2824f06d8aa50626c0ce6d634603be.exe]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre\_initialize[disablemetafiles]

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

nt\currentversion\windows[loadappinit\_dlls]

 $Queries\ value: \\ HKLM\system\currentcontrolset\control\label{likelihood} HKLM\system\currentcontrolset\control\label{likelihood} HKLM\system\currentcontrolset\control\label{likelihood} All the properties of the properties of$ 

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\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
 Queries value:
                          HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
                          HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
 Oueries value:
                          HKCU\software\microsoft\windows
nt\current version\app compatflags \hbox{$[$6b39d1b2-7883-4648-94bf-bd5109b4ac48$]}$}
                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[2a2824f06d8aa50626c0ce6d634603be.tmp]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
 Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion[commonfilesdir]
                          \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ windows nt \+ current version [registered owner]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion[registeredorganization]
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\locale[00000409]
                          HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
 Queries 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
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
 Queries value:
                          HKLM\software\microsoft\windows
\verb|nt\current| version \verb|\language| pack \verb|\surrogatefallback[plane2]|
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                          HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
 Queries 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
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
 Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]|
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
 Oueries value:
                          HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
 Oueries value:
                          HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
```

```
08002b30309d}\shellfolder[callforattributes]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[foldervalueflags]
  Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a206-a2d8-4069-a206-a206
08002b30309d}1
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\inprocserver32[]
  Queries value:
                                      HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:
\label{thm:cu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\autocomplete[append]| completion] \end{tabular}
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]
  Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
                                      HKLM\software\microsoft\com3[com+enabled]
  Queries value:
  Queries value:
                                      HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
  Oueries value:
                                      HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
  Queries value:
00c04fd7d062}\inprocserver32[]
  Queries value:
                                      HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:
                                      HKLM\software\microsoft\ole[maxsxshashcount]
                                      HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]
  Queries value:
                                      HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
  Oueries value:
00aa005b4383}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
  Oueries 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-
  Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ autocomplete \ \ []
  Queries value:
                                      HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
  Oueries value:
                                      HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
  Queries value:
b61bb7cdd997}\inprocserver32[]
  Queries value:
                                      HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
                                      HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
  Queries value:
                                      HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
HKLM\system\currentcontrol\set\control\computername[computername]
                                      HKLM\system\setup[oobeinprogress]
  Oueries value:
                                      HKLM\system\setup[systemsetupinprogress]
  Oueries value:
  Queries value:
                                      HKLM\software\microsoft\rpc[idletimerwindow]
  Oueries value:
                                      HKCU\control panel\desktop[smoothscroll]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Oueries value:
\label{thm:local_hammon} \begin{tabular}{l} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [list view shadow] \end{tabular}
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Oueries value:
                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui1
  Queries value:
                                      HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
  Oueries value:
                                      HKCU\software\microsoft\windows nt\currentversion\windows[dragdelav1]
  Oueries value:
                                      HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:
                                      HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
                                      HKCU\software\microsoft\windows
  Queries value:
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]

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

transparent bold]

Queries value:  $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} fonts ubstitutes \end{tabular} rod$ 

transparent]

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

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

new roman cyr,204]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\fontsubstitutes[helvetica]

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

ce,238]

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

shell dlg 2]

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

transparent]

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

Queries value:  $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current version + fontsubstitutes + [times + current version + current$ 

new roman tur,162]

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

transparent1

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

new roman ce.2381

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

greek,161]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\fontsubstitutes[kaiti\_gb2312]

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

HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial Oueries value: baltic,186]

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

armenian]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[fangsong\_gb2312]

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

tur,162]

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

rmn1

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

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

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

transparent1

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

nt\currentversion\fontsubstitutes[courier new baltic,186] HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times

Queries value:

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

miriam transparent]

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

shell dlg] Queries value:

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