Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 242, Task ID: 966

Task ID:	966
Risk Level:	5
Date Processed:	2016-04-28 13:14:16 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe"

Sample ID:	242
Type:	basic
Owner:	admin
Label:	d0d59c2e7bbd82b1db28d7f2d0381f4c
Date Added:	2016-04-28 12:45:15 (UTC)
File Type:	PE32:win32:gui
File Size:	897024 bytes
MD5:	d0d59c2e7bbd82b1db28d7f2d0381f4c
SHA256:	babc3284e3597c96f318c4471c7cf4995b42280471808111ca6aeb5d9cc53c92
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
5	Packer: UPX
5	PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe ["C:\windows\temp\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\Window_Washer_Rules

File System Events

Opens:	C:\Windows\Prefetch\D0D59C2E7BBD82B1DB28D7F2D0381-4106A8A8.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\d0d59c2e7bbd82b1db28d7f2d0381f4c.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_5.82.9200.16384_none_bf100cd445f4d954
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens:	C:\Windows\SysWOW64\mpr.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\sechost.dll

```
  Opens:                  C:\Windows\SysWOW64\combase.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\advapi32.dll
  Opens:                  C:\Windows\SysWOW64\user32.dll
  Opens:                  C:\Windows\SysWOW64\gdi32.dll
  Opens:                  C:\Windows\SysWOW64\ole32.dll
  Opens:                  C:\Windows\SysWOW64\oleaut32.dll
  Opens:                  C:\Windows\SysWOW64\shlwapi.dll
  Opens:                  C:\Windows\SysWOW64\shell32.dll
  Opens:                  C:\Windows\SysWOW64\iertutil.dll
  Opens:                  C:\Windows\SysWOW64\wininet.dll
  Opens:                  C:\Windows\SysWOW64\urlmon.dll
  Opens:                  C:\Windows\SysWOW64\imm32.dll
  Opens:                  C:\Windows\SysWOW64\msctf.dll
  Opens:                  C:\Windows\SysWOW64\uxtheme.dll
  Opens:                  C:\Windows\SysWOW64\dwmapi.dll
  Opens:                  C:\Languages\
  Opens:                  C:\Windows\SysWOW64\KBDUS.DLL
  Opens:                  C:\
  Opens:                  C:\recycled\
  Opens:                  C:\recycler\
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_5.82.9200.16384_en-us_d51b55b9729b0b41
  Opens:                  C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_5.82.9200.16384_en-us_d51b55b9729b0b41\comctl32.dll.mui
  Opens:                  C:\Windows\Fonts\tahoma.ttf
  Opens:                  C:\Windows\Fonts\StaticCache.dat
  Opens:                  C:\Windows\Fonts\tahomabd.ttf
  Reads from:             C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
  Opens key:              HKLM\software\microsoft\wow64
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  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\
  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:              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
  Opens key:              HKLM\software\microsoft\windows
```

```
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                 HKLM\system\currentcontrolset\control\session manager
  Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:                 HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  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:                 HKLM\
  Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:                 HKLM\system\currentcontrolset\control\networkprovider\hworder
  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:                 HKCU\software\borland\locales
  Opens key:                 HKLM\software\wow6432node\borland\locales
  Opens key:                 HKCU\software\borland\delphi\locales
  Opens key:                 HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  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:                 HKCU\software\webroot\window washer\paths
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:                 HKLM\system\currentcontrolset\control\keyboard layouts\00000409
  Opens key:                 HKCU\control panel\input method\hot keys
  Opens key:                 HKCU\control panel\input method\hot keys\00000010
  Opens key:                 HKCU\control panel\input method\hot keys\00000011
  Opens key:                 HKCU\control panel\input method\hot keys\00000012
  Opens key:                 HKCU\control panel\input method\hot keys\00000070
  Opens key:                 HKCU\control panel\input method\hot keys\00000071
  Opens key:                 HKCU\control panel\input method\hot keys\00000072
  Opens key:                 HKCU\control panel\input method\hot keys\00000104
  Opens key:                 HKCU\control panel\input method\hot keys\00000200
  Opens key:                 HKCU\control panel\input method\hot keys\00000201
  Opens key:                 HKCU\control panel\input method\hot keys\00000202
  Opens key:                 HKCU\control panel\input method\hot keys\00000203
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\netscape.exe
  Opens key:                 HKLM\software\microsoft\windows\currentversion\app paths\netscape.exe
  Opens key:                 HKCU\software\netscape\netscape navigator\biff
  Opens key:                 HKLM\software\wow6432node\netscape\netscape navigator\users
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\netscp6.exe
  Opens key:                 HKLM\software\microsoft\windows\currentversion\app paths\netscp6.exe
  Opens key:                 HKLM\software\wow6432node\netscape\netscape 6
  Opens key:                 HKLM\software\wow6432node\mozilla\netscape 6 \bin
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\netscp.exe
  Opens key:                 HKLM\software\microsoft\windows\currentversion\app paths\netscp.exe
  Opens key:                 HKLM\software\wow6432node\netscape\netscape
  Opens key:                HKLM\software\wow6432node\mozilla\netscape \bin
  Opens key:                HKLM\software\wow6432node\netscape\netscape navigator
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\aol.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\app paths\aol.exe
  Opens key:                HKLM\software\wow6432node\america online\aol\currentversion
  Opens key:                HKLM\software\wow6432node\america online\america online\4.0
  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\classes\
  Opens key:                HKCU\software\classes\appid\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe
  Opens key:                HKCR\appid\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe
  Opens key:                HKCU\software\webroot\window washer\advanced
  Opens key:                HKCU\software\classes\wow6432node\clsid\{6b38e760-d2f9-11d7-b4e1-
000347126e46}\shellid
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  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 nt\currentversion\fontlink\systemlink
  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\tahoma
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe
  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:                HKLM\software\wow6432node\microsoft\ctf\
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  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\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  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[d0d59c2e7bbd82b1db28d7f2d0381f4c.exe]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
```

```
  Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[d0d59c2e7bbd82b1db28d7f2d0381f4c]
  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\microsoft\ole[aggressivemtatesting]
  Queries value:             HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:             HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:             HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:             HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[personal]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
  Queries value:             HKLM\system\currentcontrolset\control\keyboard layouts\00000409[layout
file]
  Queries value:             HKLM\system\currentcontrolset\control\keyboard
layouts\00000409[attributes]
  Queries value:             HKCU\control panel\input method\hot keys\00000010[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000010[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000010[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000011[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000011[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000011[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000012[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000012[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000012[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000070[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000070[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000070[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000071[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000071[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000071[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000072[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000072[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000072[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000104[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000104[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000104[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000200[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000200[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000200[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000201[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000201[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000201[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000202[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000202[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000202[target ime]
  Queries value:             HKCU\control panel\input method\hot keys\00000203[virtual key]
  Queries value:             HKCU\control panel\input method\hot keys\00000203[key modifiers]
  Queries value:             HKCU\control panel\input method\hot keys\00000203[target ime]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[favorites]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[fonts]
```

```
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[nethood]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[printhood]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[programs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[sendto]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[start menu]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[startup]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[templates]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
pictures]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local settings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[content]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[mediapath]
  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\rpc[idletimerwindow]
  Queries value:              HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:              HKLM\software\microsoft\windows
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]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
```

```
  Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:                HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
  Queries value:                HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
```