# Malware Analysis Appliance by Blue Coat Systems, Inc.

### Task Details

Host: mag2, Sample ID: 619, Task ID: 2421

Task ID: 2421 Risk Level: 6

Date Processed: 2016-02-22 05:28:13 (UTC)

Processing Time: 62.71 seconds
Virtual Environment: IntelliVM

**Execution Arguments:** 

c:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe"

Sample ID: 619 Type: basic Owner: admin

Label: 81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

Date Added: 2016-02-22 05:26:49 (UTC)

File Type: PE32:win32:gui File Size: 286720 bytes

MD5: 6f2159e72e7ab7b02e18211ecbed7dd3

SHA256: 81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

Description: None

### Pattern Matching Results

1 YARA score 1

6 Modifies registry autorun entries

3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]

6 Dumps and runs batch script

5 Adds autostart object

4 Terminates process under Windows subfolder

#### Static Events

YARA rule hit: OLE2
YARA rule hit: Nonexecutable

### Process/Thread Events

Creates process:

C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
["C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe" ]

Creates process: C:\Users\Public\WinJab\winjab.exe ["C:\Users\Public\WinJab\winjab.exe"]

Creates process: C:\Windows\SysWOW64\cmd.exe [cmd /c C:\Users\Public\1.bat]

Creates process: \SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe

0xffffffff]
Terminates process:

C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe

Terminates process: C:\Windows\SysWOW64\cmd.exe
Terminates process: C:\Windows\System32\conhost.exe

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates event: \Sessions\1\BaseNamedObjects\0leDfRoot5C7031D4DAC08E93

Creates semaphore: \Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP? 81F686A320DBEC38A90D64C98861F8DDAC8BFDAA7F1AD04A8A33961283E00A22.EXE

Creates semaphore: \Sessions\1\BaseNamedObjects\C:?USERS?PUBLIC?WINJAB?WINJAB.EXE

## File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\~DF00E72943AB97A5C1.TMP

Creates: C:\Users\Public\WinJab

Creates: C:\Users\Public\WinJab\winjab.exe

C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

Creates: C:\Users\Public\1.bat

Opens: C:\Windows\Prefetch\81F686A320DBEC38A90D64C98861F-9845A13B.pf

Opens: C:\Windows

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

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

Opens:

 ${\tt C:Windows} \\ {\tt Temp} \\ {\tt 81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe} \\ {\tt execution} \\ {\tt C:Windows} \\ {\tt Temp} \\ {\tt 81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe} \\ {\tt execution} \\$ 

C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll Opens: Opens: C:\Windows\SysWOW64\KernelBase.dll C:\Windows\apppatch\sysmain.sdb Opens: C:\Windows\SysWOW64\msvbvm60.dll Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\combase.dll Opens: C:\Windows\SysWOW64\gdi32.dll Opens: Opens: C:\Windows\SysWOW64\user32.dll

```
Opens:
                         C:\Windows\SysWOW64\bcryptprimitives.dll
                         C:\Windows\SysWOW64\cryptbase.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\sspicli.dll
 Opens:
                         C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
                         C:\Windows\SysWOW64\advapi32.dll
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
 Opens:
                         C:\Windows\SysWOW64\oleaut32.dll
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\msctf.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                         C:\Windows\SysWOW64\sxs.dll
                         C:\Windows\SysWOW64\winmm.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\winmmbase.dll
                         C:\Windows\Fonts\sserife.fon
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\Windows\SysWOW64\dwmapi.dll
 Opens:
                         C:\Windows\Fonts\verdanab.ttf
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll.Config
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
 Opens:
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
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Windows\Fonts\lucon.ttf
                         C:\Windows\SysWOW64\clbcatq.dll
 Opens:
                         C:\Windows\SysWOW64\ieframe.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\SHCore.dll
 Opens:
                         C:\Windows\SysWOW64\shlwapi.dll
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\iertutil.dll
                         C:\Windows\SysWOW64\propsys.dll
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\urlmon.dll
 Opens:
                         C:\Windows\Fonts\verdana.ttf
                         C:\Windows\SysWOW64\asycfilt.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\winhttp.dll
 Opens:
                         C:\Windows\SysWOW64\nsi.dll
 Opens:
                         C:\Windows\SysWOW64\ws2_32.dll
 Opens:
                         C:\Windows\SysWOW64\webio.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
                         C:\Windows\SysWOW64\dhcpcsvc.dll
 Opens:
 Opens:
                         C:\Windows\System32\Drivers\etc\hosts
 Opens:
                         C:\Windows\SysWOW64\FWPUCLNT.DLL
                         C:\Windows\SysWOW64\en-US\mswsock.dll.mui
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wshqos.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\wshqos.dll.mui
                         C:\Windows\SysWOW64\scrrun.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\version.dll
 Opens:
                         C:\Windows\Temp
                         C:\Users\Public\WinJab\winjab.exe
 Opens:
 Opens:
                         C:\Windows\SysWOW64\ntmarta.dll
 Opens:
                         C:\Users\Public\WinJab
 Opens:
                         C: \setminus
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Public
 Opens:
                         C:\Windows\Prefetch\WINJAB.EXE-59459BCE.pf
 Opens:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
                         C:\Users\Public\1.bat
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cmd.exe
 Opens:
                         C:\Windows\WINHELP.INI
 Opens:
                         C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
 Opens:
                         C:
 Opens:
                         C:\Windows\Globalization
                         C:\Windows\Globalization\Sorting
 Opens:
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\Windows\SysWOW64\wbem
                         C: \verb|\windows\System32\ntdll.dll|\\
 Opens:
 Opens:
                         C:\Windows\System32\wow64win.dll
 Opens:
                         C:\Windows\System32\wow64cpu.dll
 Opens:
                         C:\Windows\System32\kernel32.dll
 Opens:
                         C:\Windows\System32\user32.dll
 Opens:
                         C:\Windows\System32\locale.nls
 Opens:
                         C:\Windows\SysWOW64\wbem\WMIC.exe
```

C:\Windows\SysWOW64\msvcrt.dll

Opens:

Opens: C:\Windows\System32\conhost.exe

Opens: C:\Users\Admin\AppData\Local\Temp\~DF00E72943AB97A5C1.TMP

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

Opens: C:\Windows\System32\en-US\conhost.exe.mui

Opens: C:\Windows\System32\ole32.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\System32\cmd.exe

Opens: C:\Windows\System32\en-US\cmd.exe.mui
Opens: C:\Windows\System32\dwmapi.dll

Opens: C:\Windows\System32\en-US\user32.dll.mui
Opens: C:\Windows\system32\uxtheme.dll.Config

Opens: C:\Windows\WinSxS\amd64\_microsoft.windows.common-

controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_418c2a697189c07f

Opens: C:\Windows\WinSxS\amd64\_microsoft.windows.common-controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_418c2a697189c07f\comctl32.dll

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

Opens: C:\Windows\SysWOW64\cmdext.dll
Opens: C:\Users\Public\1.bat\

Opens: C:\Windows\SysWOW64\en-US\cmd.exe.mui
Writes to: C:\Users\Public\WinJab\winjab.exe

Writes to: C:\Users\Public\1.bat

Reads from: C:\Windows\System32\Drivers\etc\hosts
Reads from: C:\Windows\SysWOW64\scrrun.dll

Reads from:

C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe

Reads from: C:\Users\Public\WinJab\winjab.exe

Reads from: C:\Users\Public\1.bat

Reads from: C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf

Deletes:

C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
Deletes: C:\Users\Admin\AppData\Local\Temp\~DF00E72943AB97A5C1.TMP

#### **Network Events**

DNS query: muzanaczekanie.pl

DNS response: muzanaczekanie.pl ⇒ 188.165.23.155

Connects to: 188.165.23.155:80

Sends data to: 0.0.0.0:53

Sends data to: muzanaczekanie.pl:80 (188.165.23.155)

Receives data from: 0.0.0.0:53

Receives data from: muzanaczekanie.pl:80 (188.165.23.155)

## Windows Registry Events

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key: HKCU\software\microsoft\windows\currentversion\run

Creates key: HKCU\software\vb and vba program settings\clock\sdata

Creates key: HKCU\software

Creates key: HKCU\software\vb and vba program settings
Creates key: HKCU\software\vb and vba program settings\clock

Opens key: HKLM\software\microsoft\wow64

Opens key: HKLM\system\currentcontrol\set\control\terminal server
Opens key: HKLM\system\currentcontrol\set\control\safeboot\option
Opens key: HKLM\system\currentcontrol\set\control\srp\gp\dll

Opens key:

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

 $Opens\ key: \\ HKLM\software\wow6432 node\microsoft\windows\currentversion\sidebyside$ 

Opens key:  ${\tt HKLM \ } {\tt System \ } {\tt Current control \ } {\tt INCLUDE} {\tt Sorting \ } {\tt Versions}$ 

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

 $\label{thm:condition} Opens \ key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ app compatflags \ disable 8 and 16 bit mitigation \\$ 

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

 $Opens\ key: \\ HKLM\software\wow6432 node\microsoft\windows\ nt\currentversion\simage\ file$ 

execution options

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

options

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

options\dllnxoptions

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

nt\currentversion\gre\_initialize

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

nt\currentversion\compatibility32

Opens key:  $\label{lem:hklm} \mbox{HKLM\software\wow6432} node\mbox{\swindows nt\currentversion\swindows} \ \ \mbox{nt\currentversion\swindows} \ \mbox{\swindows} \ \mbox{\swi$ 

compatibility

Opens key:

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\microsoft\ole

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

HKLM\software\microsoft\ole\tracing Opens kev:

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

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

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: HKLM\system\currentcontrolset\control\nls\codepage Opens key: HKLM\software\wow6432node\microsoft\vba\monitors

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus microsoft \setminus wow 6432 \\ node \setminus microsoft \setminus microsoft \setminus wow 6432 \\ node \setminus microsoft \setminus wow 6432 \\ node \setminus microsoft \setminus mic$ 

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ provider \ microsoft \ provider \ microsoft \ provider \ provider \ microsoft \ provider \ microsoft \ provider \ microsoft \ provider \ microsoft \ provider \ provider \ provider \ microsoft \ provider \ prov$ 

provider

Opens key: HKLM\software\policies\microsoft\cryptography

HKLM\software\microsoft\cryptography Opens key:

Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload

Opens key:

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

Opens key: HKCU\software\classes\ HKLM\software\microsoft\com3 Opens kev:

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

Opens key: 

00c04fd705a2}

Opens key: HKCR\activatableclasses\clsid Opens key: HKCR\activatableclasses\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}

HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens kev: 00c04fd705a2}

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2} Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key: 00c04fd705a2}\treatas

Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

00c04fd705a2}\inprocserver32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-1240a-11d0-a96b-1240a-11d0-a96b-1240a-11d0-a96b-1240a-1240a-11d0-a96b-1240a$ Opens key:

00c04fd705a2}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

00c04fd705a2}\inprochandler

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key: 00c04fd705a2}\inprochandler

Opens key:

HKLM\software\microsoft\windowsruntime\clsid\{00021401-0000-0000-c000-

000000000046}

Opens key: HKCR\activatableclasses\clsid\{00021401-0000-0000-c000-000000000046} HKCU\software\classes\wow6432node\clsid\{00021401-0000-0000-c000-Opens kev: 00000000046}

Opens key:

HKCR\wow6432node\clsid\{00021401-0000-0000-c000-000000000046} Opens key: HKCU\software\classes\wow6432node\clsid\{00021401-0000-0000-c000-000000000046}\treatas

Opens key:

HKCR\wow6432node\clsid\{00021401-0000-0000-c000-00000000046}\treatas  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00021401-0000-0000-c000-c000-c00-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c00-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c000-c$ Opens kev:

00000000046}\inprocserver32

HKCR\wow6432node\clsid\{00021401-0000-0000-c000-Opens key:

000000000046}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{00021401-0000-0000-c000-Opens key:

000000000046}\inprochandler32

HKCR\wow6432node\clsid\{00021401-0000-0000-c000-Opens kev:

00000000046}\inprochandler32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00021401-0000-0000-c000-c000-c000-c000-c00-c000-c000-c000-c000-c000-c00-c000-c000-c000-c00-$ Opens key:

000000000046}\inprochandler

HKCR\wow6432node\clsid\{00021401-0000-0000-c000-Opens key:

00000000046}\inprochandler

Opens kev: HKLM\software\wow6432node\microsoft\oleaut\userera

Opens key: HKCU\software\policies\microsoft\control

panel\international\calendars\twodigityearmax

Opens key: HKCU\control panel\international\calendars\twodigityearmax

Opens key: 

66779b670495}

Opens kev: HKCR\activatableclasses\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495} Opens key: HKCU\software\classes\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-

66779b670495}

HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\treatas

Opens key: HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-

66779b670495}\inprocserver32

HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-Opens key:

66779b670495}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-

66779b670495}\inprochandler32

HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-Opens key:

66779b670495}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-Opens key:

66779b670495}\inprochandler

HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-Opens key:

66779b670495}\inprochandler

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

settings

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

settings\winhttp

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\07a0e1d6

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9 Opens key:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ 00000005$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries

Opens key:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000001) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (cata$ 

Opens key: 

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007 Opens key:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000014 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries Opens kev:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000001$ Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000003 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000000 HKLM\software\wow6432node\microsoft\rpc

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

```
Opens key:
                                                 HKLM\system\currentcontrolset\control\computername\activecomputername
                                                 HKLM\system\setup
   Opens key:
                                                 HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows | nt\\| rpc
   Opens kev:
   Opens key:
                                                 HKLM\software\policies\microsoft\windows nt\rpc
   Opens kev:
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\connections
                                                 HKLM\system\currentcontrolset\control\cmf\config
   Opens key:
                                                 HKLM\software\policies\microsoft\peerdist\service
   Opens key:
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\peerdist\service
   Opens key:
                                                 HKLM\system\currentcontrolset\control\securityproviders
   Opens key:
                                                 HKLM\system\currentcontrolset\control\lsa\sspicache
   Opens key:
                                                 \label{lem:hklm} \verb+Kklm \+ system \+ control \+ lsa \+ spicache \+ credssp.dll
   Opens key:
                                                 HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
                                                 HKLM\system\currentcontrolset\control\sqmservicelist
   Opens key:
   Opens key:
                                                 HKLM\system\currentcontrolset\services\dnscache\parameters
                                                 HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
   Opens key:
   Opens key:
                                                 HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:
                                                 HKLM\system\currentcontrolset\services\dns
   Opens key:
                                                 HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
                                                HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
   Opens key:
   Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   Opens key:
                                                 HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
                                                 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
                                                 HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens key:
                                                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
   Opens key:
                                                \label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip6 \parameters \winsock
   Opens key:
                                                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
   Opens key:
                                                HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| system\\| dnsclient
   Opens key:
                                                 HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
HKLM \ system \ current control set \ services \ tcpip \ harameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-8
55779daa70e9}
   Opens key:
806e6f6e6963}
   Opens key:
                                                 {\tt HKLM} \verb|\system| current controlset| services| tcpip| parameters| interfaces| tcpip| and topic to
   Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
   Opens key:
25b8d56dd1d8}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
   Opens key:
                                                 HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens key:
                                                 HKCU\software\classes\scripting.filesystemobject
   Opens kev:
                                                 HKCR\scripting.filesystemobject
   Opens key:
                                                 HKCU\software\classes\scripting.filesystemobject\clsid
   Opens key:
                                                 HKCR\scripting.filesystemobject\clsid
   Opens key:
                                                 HKLM\software\microsoft\windowsruntime\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}
   Opens key:
                                                 HKCR \land ctivatable classes \land clsid \land \{0d43fe01-f093-11cf-8940-00a0c9054228\}
   Opens key:
                                                 HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}
   Opens key:
                                                 HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
   Opens key:
                                                 HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\treatas
   Opens key:
                                                 HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas
   Opens key:
                                                 HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32
   Opens key:
                                                HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32
                                                HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
   Opens key:
00a0c9054228}\inprochandler32
   Opens key:
                                                HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler32
   Opens key:
                                                00a0c9054228}\inprochandler
   Opens key:
                                                HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler
```

HKCU\software\classes\typelib Opens key: HKCR\typelib Opens key: Opens key:

HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228} Opens kev:

Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0 Opens key: Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-

00a0c9054228}\1.0\0

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0 Opens key: Opens kev: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-

00a0c9054228}\1.0\0\win32

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32 Opens key:

Opens key: HKCU\software\vb and vba program settings\clock\sdata Opens key: HKLM\software\wow6432node\policies\microsoft\windows\system

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

Opens key: 

Opens key: 

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

options\winjab.exe

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens kev: 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\winjab.exe Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\1.bat

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

options\cmd.exe

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

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

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

options\conhost.exe

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre\_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key:

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

Opens key: HKLM\software\microsoft\oleaut

HKLM\software\microsoft\windows nt\currentversion\console\truetypefont Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen

Opens key: HKCU\console HKCU\console\ Opens key:

Opens key: HKCU\console\%systemroot%\_system32\_cmd.exe Opens key: HKCU\console\%systemroot%\system32\cmd.exe

Opens key: 

Opens key: HKLM\software\microsoft\ctf\compatibility\conhost.exe HKLM\software\microsoft\windows\windows error reporting\wmr Opens kev:

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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

Opens key: HKCU\software\policies\microsoft\windows\system Opens kev: HKLM\software\wow6432node\microsoft\command processor

Opens key: HKCU\software\microsoft\command processor

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\levelobjects

Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects

Opens key:

 $HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 0 \ paths$ 

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths

Opens key:

 $HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ has hes$ 

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens kev:

Opens key:

Opens key:

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \software \policies \microsoft \windows \safer \code identifiers \parbox{0.120} ones \parbox{0.12$ Opens key:

 $HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ paths$ 

Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 4096 \ paths$ 

Opens kev:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\4096\hashes

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones

Opens key:

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths

Opens kev:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes \\$ 

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key:

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens key:

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus hashes$ Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones$ 

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus hashes$ Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes$ Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones HKLM\system\currentcontrolset\control\srp\gp\ Opens key: HKLM\system\currentcontrolset\control\srp\gp

HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Oueries value:

Opens key:

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

Queries value:

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

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

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

us[alternatecodepage]

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

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]]$ 

Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

HKCU\software\microsoft\windows Oueries value:

nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value:

options\dllnxoptions[usefilter]

```
Queries value:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[msvbvm60.dll]
    Queries value:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe]
                                                        HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value:
                                                        HKLM\software\wow6432node\microsoft\windows
nt \verb| current version \verb| compatibility 32 [81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22]| the substitution of the substituti
    Oueries value:
                                                        HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
                                                        HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
    Oueries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
    Oueries value:
                                                        HKLM\software\microsoft\ole[pageallocatorusesystemheap]
    Oueries value:
                                                        HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
    Queries value:
                                                        HKLM\software\microsoft\ole[aggressivemtatesting]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
    Oueries value:
                                                        HKLM\svstem\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]
    Oueries 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]
    Oueries value:
                                                        HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
    Queries value:
                                                        HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                                        HKLM\system\currentcontrolset\control\nls\codepage[932]
    Queries value:
                                                        Oueries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\control\nls\codepage[950]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\nls\codepage[936]
    Queries value:
                                                        HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ defaults \ provider \
provider[type]
    Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
                                                        HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
    Queries value:
    Queries value:
HKLM \verb|\software| policies \verb|\microsoft| cryptography[privkey cachepurge interval seconds]|
                                                        HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
    Queries value:
                                                        HKLM\software\microsoft\cryptography[machineguid]
    Oueries value:
    Queries value:
                                                        HKLM\software\microsoft\com3[com+enabled]
                                                        HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
    Oueries value:
    Queries value:
                                                        HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
    Queries value:
                                                        HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[1
    Queries value:
                                                        HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
                                                        HKLM\software\microsoft\ole[maxsxshashcount]
    Oueries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\control\wmi\security[5c8bb950-959e-4309-
8908-67961a1205d5]
                                                        HKCR\wow6432node\clsid\{00021401-0000-0000-c000-000000000046}[]
    Oueries value:
    Queries value:
                                                        HKCR\wow6432node\clsid\{00021401-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                                        HKCR\wow6432node\clsid\{00021401-0000-0000-c000-
    Oueries value:
000000000046}\inprocserver32[]
                                                        HKCR\wow6432node\clsid\{00021401-0000-0000-c000-
    Queries value:
00000000046}\inprocserver32[threadingmodel]
    Queries value:
                                                        HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}[]
                                                        HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-
    Queries value:
66779b670495}\inprocserver32[inprocserver32]
                                                        HKCR \verb|\wow6432| node \verb|\clsid| \{2087c2f4-2cef-4953-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8ab-4954-a8
    Queries value:
66779b670495}\inprocserver32[]
                                                        HKCR\wow6432node\clsid\{2087c2f4-2cef-4953-a8ab-
   Queries value:
66779b670495}\inprocserver32[threadingmodel]
    Queries value:
                                                        settings[sharecredswithwinhttp]
    Queries value:
                                                        settings\winhttp[disablebranchcache]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
    Queries value:
```

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007[packedcatalogitem]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerid]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
   Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[displaystring]
  Oueries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 \setminus catalog\_entries \setminus 0000000000004 [address family]]$ 

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[librarypath]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[enabled] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 numhandle buckets]$ 

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

Oueries 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]

 $Queries \ value: \\ HKLM\ software\ wow 6432 node\ microsoft\ windows\ current version\ internet$ 

settings\connections[winhttpsettings]

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\peerdist\service[enable]

Queries value:

 $\label{lem:hklm} \verb+KLM\+ system \verb+ current control \verb+ security providers [security providers] \\$ 

Queries value: HKLM\system\currentcontrol\sa\sspicache\credssp.dll[name] Queries value: HKLM\system\currentcontrol\sa\sspicache\credssp.dll[comment]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]

Queries value:HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]Queries value:HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]Queries value:HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable adapter domain name]$ 

Queries value

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [used omain named evolution]$ 

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]

Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
HKLM \verb|\system| current controlset \verb|\services| dnscache \verb|\parameters[dnstest]|
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration]
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns query time outs]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns quick query time outs]
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
  Queries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
  Oueries value:
806e6f6e6963}[enabledhcp]
  Oueries value:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-8
55779daa70e9}[registrationenabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
  Oueries value:
```

55779daa70e9}[domain]

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\}[dhcpdomain]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \currentcontrolset \services \tcpip6 \parameters \interfaces \b5105d63-74c6-4dc1-87b7-55779 \parameters \label{lem:hklmsystem} \end{subarray} \ [dhcpv6domain]$ 

Oueries value:

 $HKLM \ system \ `current control set \ `services \ 'tcpip6 \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [nameserver]$ 

Oueries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [nameserver]$ 

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [dhcpnameserver]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [registration enabled]$ 

Oueries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [register adapter name]$ 

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [dhcpdomain]$ 

Oueries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [dhcpnameserver]$ 

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [queryadaptername]$ 

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[disableadapterdomainname]

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [registration maxaddress count]$ 

Queries value:

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [queryadaptername]$ 

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [disable dynamic update]$ 

Queries value

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [registration maxaddress count]$ 

Queries value:

Queries value:

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]

Queries value: HKCR\scripting.filesystemobject\clsid[]

Queries value: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[]

Queries value: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserver32[threadingmodel]

Queries value: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[]

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus system [copyfile buffered synchronous io]$ 

Oueries value: HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension] Oueries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize] Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount] Oueries value:  $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\soften| tifiers [authenticodeen abled]$ Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[winjab.exe] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[winjab] Oueries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp] Oueries value: HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest] Oueries value: HKLM\software\microsoft\windows nt\currentversion\compatibilitv32[conhost] Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit\_dlls] HKCU\console[screencolors] Oueries value: Queries value: HKCU\console[popupcolors] Queries value: HKCU\console[insertmode] Oueries value: HKCU\console[quickedit] Queries value: HKCU\console[codepage] Queries value: HKCU\console[screenbuffersize] Oueries value: HKCU\console[windowsize] Queries value: HKCU\console[windowposition] Queries value: HKCU\console[fontsize] HKCU\console[fontfamily] Oueries value: Queries value: HKCU\console[fontweight] Queries value: HKCU\console[facename] Queries value: HKCU\console[cursorsize] HKCU\console[historybuffersize] Queries value: Queries value: HKCU\console[numberofhistorybuffers] Oueries value: HKCU\console[historynodup] HKCU\console[colortable00] Queries value: HKCU\console[colortable01] Oueries value: Oueries value: HKCU\console[colortable02] HKCU\console[colortable03] Queries value: Queries value: HKCU\console[colortable04] Oueries value: HKCU\console[colortable05] HKCU\console[colortable06] Queries value: Oueries value: HKCU\console[colortable071 Oueries value: HKCU\console[colortable08] HKCU\console[colortable09] Oueries value: HKCU\console[colortable10] Queries value: Oueries value: HKCU\console[colortable11] HKCU\console[colortable12] Queries value: Oueries value: HKCU\console[colortable131 Oueries value: HKCU\console[colortable14] Oueries value: HKCU\console[colortable15] Oueries value: HKCU\console[loadconime] Oueries value: HKCU\console[extendededitkey] Queries value: HKCU\console[extendededitkeycustom] Oueries value: HKCU\console[worddelimiters] Queries value: HKCU\console[trimleadingzeros] Oueries value: HKCU\console[enablecolorselection] Oueries value: HKCU\console[scrollscale] HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252] Oueries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable] Queries value: Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations] HKLM\software\wow6432node\microsoft\command processor[disableunccheck] Queries value: HKLM\software\wow6432node\microsoft\command processor[enableextensions] Oueries value: Oueries value: HKLM\software\wow6432node\microsoft\command processor[delayedexpansion]  $\label{local-observable} HKLM \label{local-observable} IKLM \lab$ Oueries value: Queries value: HKLM\software\wow6432node\microsoft\command processor[completionchar] Oueries value: HKLM\software\wow6432node\microsoft\command processor[pathcompletionchar] HKLM\software\wow6432node\microsoft\command processor[autorun] Oueries value: Queries value: HKCU\software\microsoft\command processor[disableunccheck] HKCU\software\microsoft\command processor[enableextensions] Oueries value: Oueries value: HKCU\software\microsoft\command processor[delayedexpansion] Oueries value: HKCU\software\microsoft\command processor[defaultcolor] Queries value: HKCU\software\microsoft\command processor[completionchar] Oueries value: HKCU\software\microsoft\command processor[pathcompletionchar]

Queries value: HKCU\software\microsoft\command processor[autorun]

Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[saferflags]

Queries value: HKLM\system\currentcontrolset\control\srp\gp[rulecount] Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} policies \end{tabular} irror of the local dentifiers \end{tabular} policies \end{tabular} irror of \end{tabula$ 

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\run[wincl]
Sets/Creates value: HKCU\software\vb and vba program settings\clock\sdata[s]