Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 3324, Task ID: 804

Task ID: 804 Risk Level: 10

2016-05-18 10:40:23 (UTC) Date Processed:

63.05 seconds Processing Time: Virtual Environment: IntelliVM

"c:\windows\temp\0fe92a59448dcd7b0d7f239c237a351e.exe" **Execution Arguments:**

3324 Sample ID: Type: basic Owner: admin

0fe92a59448dcd7b0d7f239c237a351e Label:

Date Added: 2016-05-18 10:30:50 (UTC) File Type: PE32:win32:gui:.net File Size: 44544 bytes

MD5: 0fe92a59448dcd7b0d7f239c237a351e

SHA256: 5bf14321c62ae838db535affdb9ef20949c61ee3816a222e3f610b384feaca43

Description:

Pattern Matching Results

6 Modifies registry autorun entries

3 Long sleep detected

2 .NET compiled executable

Installs service

10 Creates malicious events: Bladabindi 2 [Backdoor, RAT] 10 Creates malicious events: Bladabindi [Backdoor, RAT]

5 Creates process in suspicious location Attempts to connect to dynamic DNS

6 Checks Network Access Protection parameters

4 Reads process memory

Modifies firewall policy

6 Modifies firewall

5 Adds autostart object

4 Terminates process under Windows subfolder

Process/Thread Events

C:\WINDOWS\Temp\0fe92a59448dcd7b0d7f239c237a351e.exe Creates process:

["c:\windows\temp\0fe92a59448dcd7b0d7f239c237a351e.exe"]

Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe

["C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe"]

Creates process: C:\WINDOWS\system32\netsh.exe [netsh firewall add allowedprogram "C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe" "Trojan.exe" ENABLE]

PID:1956 C:\Program Files\Java\jre7\bin\jqs.exe Reads from process: Reads from process: PID:1416 C:\WINDOWS\system32\rundll32.exe Reads from process: PID:1148 C:\WINDOWS\system32\svchost.exe Reads from process: PID:344 C:\WINDOWS\svstem32\netsh.exe PID:1840 C:\WINDOWS\system32\wbem\unsecapp.exe Reads from process: Reads from process: PID:592 C:\WINDOWS\system32\winlogon.exe Reads from process: PID:1208 C:\WINDOWS\system32\alg.exe PID:1732 C:\WINDOWS\system32\spoolsv.exe Reads from process: PID:1068 C:\WINDOWS\system32\svchost.exe Reads from process: PID:388 C:\WINDOWS\system32\smss.exe Reads from process: PID:564 C:\WINDOWS\system32\csrss.exe Reads from process: Reads from process: PID:1896 C:\WINDOWS\explorer.exe PID:1272 C:\WINDOWS\system32\svchost.exe Reads from process: Reads from process: PID:292 C:\WINDOWS\system32\ctfmon.exe

Reads from process: PID:540 C:\WINDOWS\system32\wbem\wmiprvse.exe PID:908 C:\WINDOWS\system32\lsass.exe Reads from process:

Reads from process: PID:272 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe

Reads from process: PID:896 C:\WINDOWS\system32\services.exe Reads from process: PID:1340 C:\WINDOWS\system32\svchost.exe

Terminates process: C:\WINDOWS\Temp\0fe92a59448dcd7b0d7f239c237a351e.exe

Terminates process: C:\WINDOWS\system32\netsh.exe

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-Creates mutex:

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

\BaseNamedObjects\ZonesCounterMutex Creates mutex:

Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex

```
\BaseNamedObjects\SHIMLIB_LOG_MUTEX
       Creates mutex:
                                                                                             \BaseNamedObjects\5cd8f17f4086744065eb0992a09e05a2
     Creates mutex:
      Creates mutex:
                                                                                              \BaseNamedObjects\.net clr networking
     Creates event:
                                                                                             \BaseNamedObjects\CorDBIPCSetupSyncEvent_300
                                                                                             \BaseNamedObjects\CorDBIPCSetupSyncEvent_304
      Creates event:
      Creates event:
                                                                                             \BaseNamedObjects\userenv: User Profile setup event
      Creates semaphore:
                                                                                              \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
                                                                                              \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
      Creates semaphore:
     Creates semaphore:
                                                                                            \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
File System Events
      Creates:
                                                                                            C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe
     Creates:
                                                                                            C:\Documents and Settings\Admin\Start
 Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
      Creates:
                                                                                            C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe.tmp
                                                                                            C:\WINDOWS\Prefetch\0FE92A59448DCD7B0D7F239C237A3-39AB25B2.pf
      Opens:
      Opens:
                                                                                            C:\Documents and Settings\Admin
      Opens:
                                                                                            C:\WINDOWS\system32\mscoree.dll
      Opens:
                                                                                            C:\WINDOWS\system32\imm32.dll
                                                                                            C:\windows\temp\0fe92a59448dcd7b0d7f239c237a351e.exe.config
      Opens:
                                                                                            C:\WINDOWS\Temp\0fe92a59448dcd7b0d7f239c237a351e.exe
      Opens:
      Opens:
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
      Opens:
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
                                                                                            \label{lem:c:windows} C: \verb|\windows| Microsoft.NET\Framework| v2.0.50727 \verb|\windows| anifest | lem to the constant of the co
      Opens:
      Opens:
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Config
      Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
      Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcr80.dll
      Opens:
                                                                                            C:\WINDOWS
      Opens:
      Opens:
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config
      Opens:
                                                                                            \label{lem:config} C: \WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
      Opens:
     Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
                                                                                            C:\WINDOWS\system32\shell32.dll
      Opens:
      Opens:
                                                                                            C:\WINDOWS\system32\shell32.dll.124.Manifest
      Opens:
                                                                                            C:\WINDOWS\system32\shell32.dll.124.Config
     Opens:
                                                                                            C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                                                                                            C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                                                                                            C:\WINDOWS\WindowsShell.Manifest
      Opens:
                                                                                            C:\WINDOWS\WindowsShell.Config
      Opens:
      Opens:
                                                                                            C:\WINDOWS\system32\comctl32.dll
      Opens:
                                                                                            C:\WINDOWS\system32\comctl32.dll.124.Manifest
      Opens:
                                                                                            C:\WINDOWS\system32\comctl32.dll.124.Config
                                                                                            C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
      Opens:
Config\v2.0.50727.42\security.config
      Opens:
                                                                                            C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
Config\v2.0.50727.42\security.config.cch
       Opens:
                                                                                            C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\index9c.dat
      Opens:
C: \verb|WINDOWS| assembly \verb|NativeImages_v2.0.50727_32 \verb| mscorlib| adb89 fa22 fd5b4ce433b5aca7fb1b07 \verb| mscorlib.ni.dll| adb89 fa22 fd5b4ce433b5aca7fb1b07 \verb| mscorlib.ni.dll| abb89 fa22 fd5b4ce43aca7fb1b07 abb89 fa2
                                                                                            C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089
      Opens:
                                                                                            C:\WINDOWS\Temp
      Opens:
      Opens:
                                                                                            C:\WINDOWS\system32\rpcss.dll
                                                                                            C:\WINDOWS\system32\MSCTF.dll
      Opens:
      Opens:
                                                                                            C:\WINDOWS\system32\l_intl.nls
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
      Opens:
      Opens:
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscoriit.dll.2.Manifest
      Opens:
                                                                                            C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll.2.Config
      Opens:
                                                                                            C:\WINDOWS\assembly\pubpol1.dat
      Opens:
C: \verb|WINDOWS| assembly \verb|NativeImages_v2.0.50727_32 \verb|System| aa7926460a336408c8041330ad90929d \verb|System.ni.dll| additionally a simple of the control of th
      Opens:
C: \windows \assembly \native Images\_v2.0.50727\_32 \mbox{\sc first-visualBas+\sb3d048d8c003d743ea5e72caf07773a\mbox{\sc microsoft.} VisualBasic.ni.dll \native Images\_v2.0.50727\_32 \mbox{\sc microsoft.} VisualBasic.ni.dll \na
      Opens:
C:\WINDOWS\assembly\GAC_MSIL\Microsoft.VisualBasic\8.0.0.0_b03f5f7f11d50a3a
       Opens:
                                                                                            C:\WINDOWS\assembly\GAC_MSIL\System\2.0.0.0_b77a5c561934e089
      Opens:
C: \verb|WINDOWS| assembly \verb|NativeImages_v2.0.50727_32| System.Drawing \verb|6978f2e90f13bc720d57fa6895c911e2| System.Drawing.ni.dll | System.Drawing to the content of the cont
     Opens:
C: \windows. Forms. \yindows. \y
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089
      Opens:
                                                                                            C:\WINDOWS\assembly\GAC_MSIL\System.Drawing\2.0.0.0_b03f5f7f11d50a3a
      Opens:
C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089\sorttbls.nlp
      Opens:
C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089\sortkey.nlp
```

Opens:

Opens:

C:\Documents and Settings

C:\Documents and Settings\Admin\Local Settings\Temp

```
Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\All Users
                         C:\Documents and Settings\All Users\Documents\desktop.ini
 Opens:
                         {\tt C:\WINDOWS\system32\clbcatq.dll}
 Opens:
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\urlmon.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe.Manifest
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe.Config
 Opens:
 Opens:
                         C:\WINDOWS\Prefetch\TROJAN.EXE-24702E36.pf
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe.config
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
 Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.300.64803
 Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.300.64803
                         C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
 Opens:
Config\v2.0.50727.42\security.config.cch.300.64833
                         C:\WINDOWS\system32\netsh.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS\system32\netsh.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\NETSH.EXE-085CFFDE.pf
 Opens:
                         C:\WINDOWS\system32\shfolder.dll
 Opens:
                         C:\WINDOWS\svstem32\mprapi.dll
 Opens:
                         C:\WINDOWS\system32\activeds.dll
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Startup
 Opens:
                         C:\WINDOWS\system32\adsldpc.dll
 Opens:
                         C:\WINDOWS\system32\atl.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\samlib.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\winmm.dll
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
                         C:\WINDOWS\AppPatch\AcGenral.dll
 Opens:
                         C:\WINDOWS\system32\msacm32.dll
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\ipv6mon.dll
 Opens:
                         C:\WINDOWS\system32\xpob2res.dll
 Opens:
                         C:\WINDOWS\system32\ipmontr.dll
 Opens:
                         C:\WINDOWS\system32\ifmon.dll
 Opens:
                         C:\WINDOWS\system32\netcfgx.dll
 Opens:
                         C:\WINDOWS\system32\clusapi.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\svstem32\netshell.dll
 Opens:
                         C:\WINDOWS\system32\credui.dll
 Opens:
                         C:\WINDOWS\system32\dot3api.dll
 Opens:
                         C:\WINDOWS\system32\dot3dlg.dll
 Opens:
                         C:\WINDOWS\system32\onex.dll
 Opens:
                         C:\WINDOWS\system32\wtsapi32.dll
 Opens:
                         C:\WINDOWS\system32\winsta.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\msasn1.dll
 Opens:
                         C:\WINDOWS\system32\eappcfg.dll
 Opens:
                         C:\WINDOWS\system32\msvcp60.dll
 Opens:
                         C:\WINDOWS\system32\eappprxy.dll
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\svstem32\psapi.dll
 Opens:
                         C:\WINDOWS\system32\netshell.dll.50.Manifest
 Opens:
                         C:\WINDOWS\system32\netshell.dll.50.Config
 Opens:
                         C:\WINDOWS\system32\ippromon.dll
 Opens:
                         C:\WINDOWS\system32\rasmontr.dll
 Opens:
                         C:\WINDOWS\system32\ipxmontr.dll
 Opens:
                         C:\WINDOWS\system32\ipxpromn.dll
 Opens:
                         C:\WINDOWS\system32\dgnet.dll
 Opens:
                         C:\WINDOWS\system32\wbem\framedyn.dll
 Opens:
                         C:\WINDOWS\system32\wbem\wbemprox.dll
                         C:\WINDOWS\system32\wbem\wbemcomn.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\hnetmon.dll
 Opens:
                         C:\WINDOWS\system32\fwcfg.dll
```

```
C:\WINDOWS\system32\napmontr.dll
Opens:
Opens:
                        C:\WINDOWS\system32\qutil.dll
Opens:
                        C:\WINDOWS\system32\dot3cfg.dll
```

C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe.tmp Opens:

Opens: C:\WINDOWS\system32\qagent.dll

Opens:

Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll Opens: C:\WINDOWS\system32\wbem\fastprox.dll C:\WINDOWS\system32\ntdsapi.dll Opens: Opens:

C:\WINDOWS\assembly\GAC_MSIL\System.Configuration\2.0.0.0_b03f5f7f11d50a3a

C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Xml\36f3953f24d4f0b767bf172331ad6f3e\System.Xml.ni.dll

C:\WINDOWS\assembly\GAC_MSIL\System.Xml\2.0.0.0_b77a5c561934e089 Opens:

C:\WINDOWS\Temp\d39cb9f7-780e-4439-9461-4f41bca9b7b3 Opens:

C:\WINDOWS\system32\hnetcfg.dll Opens: Opens: C:\WINDOWS\system32\wshtcpip.dll Opens: C:\WINDOWS\system32\drivers\etc\hosts Opens: C:\WINDOWS\system32\rsaenh.dll C:\WINDOWS\system32\rasadhlp.dll Opens:

 ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Trojan.exe}$ Writes to:

Writes to: C:\Documents and Settings\Admin\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe

Writes to: ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Trojan.exe.tmp}$ Reads from: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

C:\Documents and Settings\Admin\My Documents\desktop.ini Reads from: Reads from: C:\Documents and Settings\All Users\Documents\desktop.ini

Reads from: C:\WINDOWS\Registration\R00000000007.clb

Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe

C:\WINDOWS\system32\drivers\etc\hosts Reads from: Reads from: C:\WINDOWS\system32\rsaenh.dll

Network Events

almashaks70.no-ip.org DNS query:

Sends data to: 8.8.8.8:53 Receives data from: 0.0.0.0:0

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders

Creates key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default$

Creates key: HKCU\software\5cd8f17f4086744065eb0992a09e05a2

Creates key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-

806d6172696f}\

Creates kev: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders

Creates key: HKCU\software\microsoft\multimedia\audio

HKCU\software\microsoft\multimedia\audio compression manager\ Creates kev: Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority

v4.00

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Creates key: HKLM\software\microsoft\windows nt\currentversion\tracing

Creates key: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\tracing\microsoft\eappcfg|$ HKLM\software\microsoft\windows Creates kev: nt\currentversion\tracing\microsoft\eappcfg\traceidentifier HKLM\software\microsoft\windows Creates key:

nt\currentversion\tracing\microsoft\eappprxy

Creates key: HKLM\software\microsoft\windows nt\currentversion\tracing\microsoft\eappprxy\traceidentifier HKLM\software\microsoft\wbem\cimom Creates key: Creates key: HKLM\software\microsoft\windows

nt\currentversion\tracing\microsoft\qutil HKLM\software\microsoft\windows Creates kev: nt\currentversion\tracing\microsoft\qutil\traceidentifier HKLM\software\microsoft\tracing Creates key: Creates key: HKLM\software\microsoft\windows nt\currentversion\tracing\microsoft\nap\netsh

Creates key: HKLM\software\microsoft\windows nt\currentversion\tracing\microsoft\nap\netsh\napmontr HKLM\software\microsoft\windows Creates key:

 $\verb|nt\currentversion\tracing\microsoft\qagent|$

HKLM\software\microsoft\windows Creates key: nt\currentversion\tracing\microsoft\qagent\traceidentifier

Creates key: HKLM\system\currentcontrolset\services\napagent\localconfig

Creates key:

HKLM\system\currentcontrolset\services\napagent\localconfig\enroll\hcsgroups Creates kev: HKLM\svstem\currentcontrolset\services\napagent\shas Creates key: HKLM\svstem\currentcontrolset\services\napagent\gecs

Creates key: HKLM\system\currentcontrolset\services\napagent\localconfig\ui

Creates key:

```
Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\0fe92a59448dcd7b0d7f239c237a351e.exe
 Opens kev:
                      HKLM\system\currentcontrolset\control\safeboot\option
 Opens key:
                      HKLM\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                      HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                      HKLM\system\currentcontrolset\control\terminal server
 Opens key:
                      HKLM\system\currentcontrolset\control\session manager
 Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
 Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
 Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
 Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\winlogon
 Opens key:
                      HKLM\
```

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ diagnostics$ Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\kernel32.dll

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

options\mscoree.dll

Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKLM\software\microsoft\.netframework

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

options\user32.dll

Opens key:

 ${\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}$ options\imm32.dll

Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant of th$

options\gdi32.dll

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

options\msvcrt.dll

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

options\shlwapi.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus ime \ compatibility}$ Opens key: HKLM\software\microsoft\windows nt\currentversion\windows

Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ performance$

Opens key: HKCU\

Opens key: HKCU\software\microsoft\.netframework\policy\standards Opens key: HKLM\software\microsoft\.netframework\policy\standards

 $HKLM \verb|\software\microsoft|.netframework\policy\standards\v2.0.50727$ Opens key:

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

Opens key: HKCU\control panel\desktop

Opens key:

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

Opens key: $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc file\ execution} \\$

options\msvcr80.dll

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

options\mscorwks.dll

Opens key: HKCU\software\microsoft\.netframework Opens key: HKLM\software\microsoft\fusion HKCU\software\microsoft\fusion Opens key:

Opens key:

HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet

Opens key:

 $HKLM \label{lem:hklm} White the temperature of the second of the secon$ Opens key:

1757981266-507921405-1957994488-1003

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

options\shell32.dll

Opens kev: HKLM\svstem\setup

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

options\comctl32.dll

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ language pack$ Opens key: HKLM\software\microsoft\.netframework\v2.0.50727\security\policy Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c Opens kev: Opens key:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 8100e2c5 \setminus 181938c6 \setminus 191938c6 \setminus 191936c6 \setminus 1919$

Opens key:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 7950e2c5 \ 3838a3a4 \ 888a3a4 \ and \ barried \ and \ and$

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

options\ole32.dll

Opens key: HKLM\software\microsoft\ole

Opens kev: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}

Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ options\mscorlib.ni.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll Opens kev: Opens key: HKLM\software\microsoft\ctf\systemshared\ Opens key: HKCU\keyboard layout\toggle Opens key: HKLM\software\microsoft\ctf\ Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\77\20f75277 $\label{lem:hklm} \verb+Kklm \software \verb+microsoft \ framework setup \verb+\dotnetclient \v3.5+ \\$ Opens key: Opens key: HKLM\software\microsoft\strongname Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mscorjit.dll Opens key: HKLM\software\microsoft\fusion\publisherpolicy\default Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus ni \setminus 1c22df2f \setminus 4f99a7c9$ Opens kev $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 1c22 df2f \ 1d9a7c9 \ 3f \ ni \ 1c22 df2f \ 1d9a7c9 \ 1d2 df2f \ 1d2 d$ Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 6dc7d4c0\ 7cd935b4\ extra \ part \ fusion \ part \ fusion \ part \$ Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5\ 32e43dd1\ description \ and \ analyze \ and \ analyze \ analyze$ Opens key: Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 2b1a4e4 \ 502472a2 \ 3e$ Opens key: Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 4f99a7c9 \setminus 340b8570 \setminus 4f$ Opens kev $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni\ 30bc7c4f\ 3f50fe4f\ 7f50fe4f\ 7f5$ Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ i1\ 424bd4d8 \ 2bfe65de \ 5de \ 5de$ Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6 Opens kev: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ i1\ 3f50fe4f\ 7540f5be\ 754$ HKLM\software\microsoft\.netframework\policy\aptca Opens key: Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus ni \setminus 61e7e666 \setminus c991064$ Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus ni \setminus 61e7e666 \setminus c991064 \setminus 13e9666 \setminus c991066 \setminus c$ Opens key: Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30 Opens key: $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ v2.0.50727_32 \ il\ 41c04c7e\ 286a445d\ 24ex \ native images in dex \ native images in d$ Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17 HKCU\software\5cd8f17f4086744065eb0992a09e05a2 Opens key: Opens key: HKCU\environment Opens key: HKCU\software\microsoft\windows\currentversion\explorer HKLM\software\microsoft\windows\currentversion\explorer Opens key: Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ options\netapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\system.ni.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\microsoft.visualbasic.ni.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ options\system.drawing.ni.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\system.windows.forms.ni.dll HKLM\software\microsoft\rpc\pagedbuffers Opens key: Opens key: HKLM\software\microsoft\rpc Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\0fe92a59448dcd7b0d7f239c237a351e.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: Opens key:

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32

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

Opens key: HKCR\drive\shellex\folderextensions

HKCU\software\classes\

HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

a2d8-08002b30309d} Opens key:

Opens key:

HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-Opens key: 4442-804e-409d6c4515e9} Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9} Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|.exe| \\ \end{tabular}$ Opens key: HKCU\software\classes\.exe Opens key: HKCR\.exe Opens key: HKCU\software\classes\exefile Opens kev: HKCR\exefile HKCU\software\classes\exefile\curver Opens key: Opens key: HKCR\exefile\curver Opens key: HKCR\exefile\ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: HKCU\software\microsoft\windows\currentversion\policies\system HKCU\software\classes\exefile\shellex\iconhandler Opens key: Opens kev: HKCR\exefile\shellex\iconhandler Opens key: HKCU\software\classes\systemfileassociations\.exe Opens key: HKCR\systemfileassociations\.exe Opens key: HKCU\software\classes\systemfileassociations\application Opens key: HKCR\systemfileassociations\application Opens key: HKCU\software\classes\exefile\clsid HKCR\exefile\clsid Opens key: Opens key: HKCU\software\classes* Opens key: HKCR* Opens key: HKCU\software\classes*\clsid Opens key: HKCR*\clsid Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.dll Opens key: HKLM\system\currentcontrolset\control\minint Opens key: HKLM\system\wpa\pnp Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\microsoft\windows\currentversion Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\policies\microsoft\system\dnsclient Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume Opens kev: 11e3-9fc7-806d6172696f}\ Opens key: HKCU\software\classes\directory Opens key: HKCR\directory Opens key: HKCU\software\classes\directory\curver Opens key: HKCR\directorv\curver Opens key: HKCR\directory\ HKCU\software\classes\directory\shellex\iconhandler Opens key: Opens key: HKCR\directory\shellex\iconhandler HKCU\software\classes\directory\clsid Opens key: Opens key: HKCR\directory\clsid

HKCU\software\classes\folder Opens key:

Opens key: HKCR\folder

Opens key: HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid

Opens kev:

HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks

Opens kev: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-

00c04fd91972}\inprocserver32

 $HKCR \clsid \aeb6717e-7e19-11d0-97ee-00c04fd91972 \hiprocserver 32$ Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\policies\associations Opens key: HKCU\software\microsoft\windows\currentversion\policies\associations

Opens key: HKCU\software\classes\.ade

Opens kev: HKCR\.ade

HKCU\software\classes\.adp Opens key:

Opens key: HKCR\.adp

HKCU\software\classes\.app Opens key:

Opens key: HKCR\.app

Opens key: HKCU\software\classes\.asp

Opens kev: HKCR\.asp

Opens key: HKCU\software\classes\.bas

Opens key: HKCR\.bas

Opens key: HKCU\software\classes\.bat HKCR\.bat

Opens key: Opens key:

HKCU\software\classes\.cer

Opens key: HKCR\.cer

HKCU\software\classes\.chm Opens key: Opens key: HKCR\.chm Opens key: HKCU\software\classes\.cmd

Opens key: HKCR\.cmd

Opens key: HKCU\software\classes\.com

Opens key: HKCR\.com

Opens key: HKCU\software\classes\.cpl

Opens key: HKCR\.cpl Opens key: HKCU\software\classes\.crt

Opens key: HKCR\.crt HKCU\software\classes\.csh Opens kev:

Opens key: HKCR\.csh

HKLM\software\microsoft\com3 Opens key:

Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant of th$ options\comres.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\oleaut32.dll Opens key: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll Opens key: HKLM\software\microsoft\com3\debug Opens key: HKLM\software\classes Opens key: HKU\ Opens key: HKCR\clsid Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32 HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32 Opens key: Opens key HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86 Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86 Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32 Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32 Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32$ Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key: 00c04fb6bfc4}\inprochandlerx86 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86$ Opens kev: Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver Opens key: $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll Opens key: HKCU\software\classes\protocols\name-space handler\ Opens key: HKCR\protocols\name-space handler Opens key: HKCU\software\classes\protocols\name-space handler Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature protocol lockdown HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\ Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature unc savedfilecheck HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 Opens key: HKLM\software\policies Opens key: HKCU\software\policies Opens key: HKCU\software Opens key: HKLM\software Opens kev: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\

HKCU\software\microsoft\windows\currentversion\internet

Opens key:

```
settings\zonemap\protocoldefaults\
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                      HKLM\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\domains\
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com\related
                                      HKCU\software\microsoft\internet
  Opens kev:
explorer \verb|\main\featurecontrol\feature\_use\_ietldlist\_for\_domain\_determination| \\
  Opens key:
                                      HKLM\software\microsoft\internet
\hbox{\tt explorer} \\ \hbox{\tt main} \\ \hbox{\tt featurecontrol} \\ \hbox{\tt feature\_use\_ietldlist\_for\_domain\_determination} \\
  Opens key:
                                      HKCU\software\microsoft\internet explorer\ietld
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
                                      HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature allow reverse solidus in userinfo kb932562
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer\security
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens key:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\zones\endown} \mbox{\tt 2} \mbox{\tt ones\scale} \mbox{\tt 0} \mbox{\tt ones\scale} \mbox{\tt on
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
                                      HKLM \verb|\software\policies\microsoft\windows\currentversion\ | internet
settings\zones\
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones\0
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\0
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key
settings\zones\4
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
  Opens key:
settings\zones\4
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev
settings\lockdown_zones\1
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\2
  Opens key:
                                      \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\2
  Opens kev:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\lockdown_zones\3
   Opens key:
                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\3
   Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
    Opens key:
                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\4
                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\4
                                                              HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature zones default drive intranet kb941000
    Opens key:
                                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature zones default drive intranet kb941000
    Opens key:
                                                             HKCU\software\classes\exefile\shell
    Opens key:
                                                              HKCR\exefile\shell
    Opens key:
                                                              HKCU\software\classes\exefile\shell\open
    Opens key:
                                                              HKCR\exefile\shell\open
    Opens key:
                                                              HKCU\software\classes\exefile\shell\open\command
    Opens key:
                                                              HKCR\exefile\shell\open\command
    Opens key:
HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun
    Opens key:
                                                              HKLM\software\microsoft\windows\currentversion\app paths\trojan.exe
    Opens key:
                                                              HKCU\software\classes\exefile\shell\open\ddeexec
    Opens key:
                                                              HKCR\exefile\shell\open\ddeexec
    Opens key:
                                                              HKCU\software\classes\applications\troian.exe
    Opens key:
                                                              HKCR\applications\trojan.exe
    Opens key:
                                                              HKCU\software\microsoft\windows\shellnoroam
    Opens key:
                                                              HKCU\software\microsoft\windows\shellnoroam\muicache
    Opens key:
                                                              HKCU\software\microsoft\windows\shellnoroam\muicache\
    Opens key:
                                                              Opens kev:
                                                              HKLM\system\currentcontrolset\control\session manager\appcertdlls
    Opens key:
                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
    Opens key:
                                                              HKLM\system\wpa\tabletpc
    Opens key:
                                                              HKLM\system\wpa\mediacenter
    Opens key:
                                                              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
                                                              HKLM\software\microsoft\windows
    Opens kev:
nt\currentversion\appcompatflags\custom\trojan.exe
    Opens key:
                                                              HKLM\software\policies\microsoft\windows\safer\levelobjects
                                                              HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
    Opens key:
    Opens key:
be2efd2c1a33}
    Opens key:
                                                              HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
    Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57
b813f72dbb91}
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
    Opens key:
HKLM \ software \ \ microsoft \ \ windows \ \ safer \ \ \ deidentifiers \ \ \ 4096 \ \ paths
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
   Opens key:
HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers \verb|\software| length of the microsoft \|\software| length of the microsoft \|\soft
    Opens kev
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
    Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus has hes
    Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
    Opens key:
                                                              \label{lem:hkcu} \label{lkcu} HKCU software \policies \microsoft \windows \safer \code identifiers \normalised \policies \microsoft \windows \safer \code identifiers \normalised \policies \polic
```

```
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
       Opens key:
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
      Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
      Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
      Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
      Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \code ident
      Opens key:
                                                                                                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
      Opens key:
                                                                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\trojan.exe
      Opens key:
                                                                                                 HKLM\software\microsoft\ctf\compatibility\trojan.exe
      Opens key:
                                                                                                 HKCU\software\classes\appid\0fe92a59448dcd7b0d7f239c237a351e.exe
      Opens kev:
                                                                                                HKCR\appid\0fe92a59448dcd7b0d7f239c237a351e.exe
      Opens kev:
                                                                                                HKLM\svstem\currentcontrolset\control\lsa
     Opens key:
                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
      Opens key:
                                                                                                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\netsh.exe
                                                                                                HKLM\software\microsoft\windows nt\currentversion\appcompatflags
      Opens kev:
                                                                                                HKCU\software\microsoft\windows nt\currentversion\appcompatflags
      Opens kev:
      Opens key:
                                                                                                \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options\netsh.exe
                                                                                                 HKCU\software\microsoft\windows\currentversion\run
      Opens key:
      Opens key:
                                                                                                 HKLM\software\microsoft\windows\currentversion\run
                                                                                                \label{lem:hklmsoftware} \mbox{\sc hklmsoftware\sc microsoft\sc micr
     Opens key:
options\shfolder.dll
      Opens key:
                                                                                                \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options\acgenral.dll
      Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
      Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\adsldpc.dll
      Opens key:
                                                                                                 \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant of th
options\atl.dll
      Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\activeds.dll
     Opens kev:
                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
     Opens key:
                                                                                                 {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}
options\samlib.dll
      Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mprapi.dll
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\ws2help.dll
      Opens key:
                                                                                                 {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}
options\ws2_32.dll
     Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens kev:
options\winmm.dll
      Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
     Opens key:
                                                                                                 \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant of th
options\rasapi32.dll
      Opens key:
                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
      Opens key:
                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
     Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
                                                                                                 {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}
     Opens key:
options\userenv.dll
      Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
      Opens key:
                                                                                                 HKLM\system\currentcontrolset\services\ldap
      Opens kev:
                                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32
      Opens key:
```

Opens key: HKLM\software\microsoft\windows\currentversion\telephony Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\ Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces Opens key: HKLM\system\currentcontrolset\services\netbt\parameters Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache$ Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm $HKLM \ \ software \ \ \ microsoft \ \ \ audio compression manager \ \ \ \ msacm. \ msg711$ Opens key: Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610 Opens key: $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wicrosoft \label{lem:hklm} audio compression manager \label{lem:hklm} driver cache \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hkklm} \label{lem:hklm} \label{lem:hkklm} \label{le$ Opens key: $HKLM \verb|\software\microsoft\audiocompression manager\driver cache \verb|\msacm.msg723| \\$ Opens key: $HKLM \ \ software \ \ \ microsoft \ \ \ audio compression manager \ \ \ driver cache \ \ msaudio 1$ Opens kev HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm Opens key: HKLM\system\currentcontrolset\control\productoptions Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens key: HKLM\software\policies\microsoft\windows\system Opens kev: HKCU\software\microsoft\windows\currentversion\thememanager HKLM\software\microsoft\netsh Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ipv6mon.dll Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: Opens kev HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004 Opens key: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries$ Opens key: Opens kev: 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 key Opens key: Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens kev: Opens key: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog_entries \ 000000000011$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ 00000004$ Opens key: Opens key: Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ipmontr.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\trojan.exe\rpcthreadpoolthrottle $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the$ Opens kev options\clusapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psapi.dll Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netcfgx.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\credui.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$

```
options\dot3api.dll
   Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winsta.dll
   Opens kev:
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
   Opens key:
                                                           {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}
options\msasn1.dll
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
   Opens key:
                                                           HKLM\svstem\currentcontrolset\services\crvpt32\performance
                                                          \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \begin{tabular}{ll} software \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows & nt \current version \begin{tabular}{ll} microsoft \begin{tabular}{ll} micro
    Opens key:
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
    Opens key:
                                                           \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant of th
options\eappcfg.dll
   Opens key:
                                                           HKLM\system\currentcontrolset\control\wmi\security
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\eappprxy.dll
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\onex.dll
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\dot3dlg.dll
    Opens key:
                                                           {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}
options\netshell.dll
   Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
    Opens kev:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ifmon.dll
   Opens key:
                                                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\ippromon.dll
   Opens key:
                                                           \label{lem:hklmsoftware} $$HKLM\software\microsoft\windows nt\currentversion\image file execution $$
options\rasmontr.dll
   Opens key:
                                                          HKLM\software\microsoft\windows nt\currentversion
   Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ipxmontr.dll
    Opens key:
                                                           \label{lem:hklmsoftware} $$HKLM\software\microsoft\windows nt\currentversion\image file execution $$
options\ipxpromn.dll
   Opens key:
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\framedyn.dll
   Opens kev:
                                                           HKLM\software\microsoft\wbem\cimom
    Opens key:
                                                          \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options\dgnet.dll
                                                           {\tt HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus netsh. exe}
    Opens key:
    Opens key:
                                                           HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
    Opens key:
                                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
    Opens key:
                                                          00aa004b2e24}\treatas
    Opens key:
                                                          HKCR\clsid{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
    Opens key:
                                                          HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
                                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
    Opens key:
                                                          Opens key:
00aa004b2e24}\inprocserverx86
    Opens key:
                                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86
                                                          HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
    Opens key:
00aa004b2e24}\localserver32
    Opens key:
                                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32
                                                          Opens key:
00aa004b2e24}\inprochandler32
                                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
    Opens key:
                                                          HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
    Opens key
00aa004b2e24}\inprochandlerx86
                                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
    Opens key:
    Opens key:
                                                          HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\localserver
                                                           HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver
    Opens key:
    Opens key:
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemcomn.dll
   Opens kev:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemprox.dll
    Opens key:
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetmon.dll
   Opens key:
                                                           \label{lem:hklmsoftware} $$HKLM\software\microsoft\windows nt\currentversion\image file execution $$
options\fwcfg.dll
    Opens key:
                                                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\qutil.dll
   Opens key:
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\napmontr.dll
   Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dot3cfg.dll
    Opens key:
                                                           HKLM\software\microsoft\tracing\fwcfg
                                                           Opens key:
    Opens key:
                                                           HKLM\software\microsoft\cryptography\defaults\provider\gemplus gemsafe
card csp v1.0
    Opens key:
                                                           HKLM\software\microsoft\cryptography\defaults\provider\infineon sicrypt
base smart card csp
   Opens key
                                                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
```

cryptographic provider v1.0

```
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} If the lem is a second constant of the lem is a second constant
  Opens key:
dss and diffie-hellman cryptographic provider
  Opens key:
                                   HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
dss cryptographic provider
                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ dh
  Opens key:
schannel cryptographic provider
                                  Opens key:
enhanced cryptographic provider v1.0
                                  {\tt HKLM \coftware \microsoft \cryptography \defaults \provider \microsoft}
  Opens key
enhanced dss and diffie-hellman cryptographic provider
  Opens key:
                                  enhanced rsa and aes cryptographic provider (prototype)
                                  HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa
  Opens kev
schannel cryptographic provider
  Opens key
                                  HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:
                                  HKLM\software\microsoft\cryptography\defaults\provider\schlumberger
cryptographic service provider
  Opens key:
                                   HKLM\software\microsoft\cryptography\oid
  Opens key:
                                  HKLM\software\microsoft\cryptography\oid\encodingtype 0
                                  HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
0\cryptdllfindoidinfo
  Opens key:
                                   HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}
  Opens key:
                                   HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}
  Opens key:
                                   HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\treatas
                                  HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\treatas
  Opens kev:
                                  HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
  Opens key:
28ecbd96ba8c}\inprocserver32
  Opens key:
                                  HKCR\clsid\\ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c\\\inprocserver32
  Opens key:
                                   HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprocserverx86
  Opens kev:
                                  HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprocserverx86
  Opens key:
                                  HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\localserver32
  Opens key:
                                  HKCR\clsid\\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\\\localserver32
                                   Opens key:
28ecbd96ba8c}\inprochandler32
                                  HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprochandler32
  Opens kev:
                                  HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
  Opens kev
28ecbd96ba8c}\inprochandlerx86
                                  HKCR\clsid\\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\\{inprochandlerx86}
  Opens key:
                                  HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
  Opens key:
28ecbd96ba8c}\localserver
                                  HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\localserver
  Opens key:
  Opens key:
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\qagent.dll
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8
  Opens key:
Opens key:
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netsh.exe\rpcthreadpoolthrottle
  Opens key:
                                  HKLM\system\currentcontrolset\services\napagent\localconfig\
  Opens kev
HKLM\system\currentcontrolset\services\napagent\localconfig\enroll\hcsgroups\
  Opens key:
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}
  Opens key:
                                  HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}
  Opens key:
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\treatas
  Opens key:
                                  HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\treatas
  Opens key:
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprocserver32
  Opens key:
                                  HKCR \clsid \eb082ba1-df8a-46be-82f3-35bf9e9be52f\} \label{eb082ba1-df8a-46be-82f3-35bf9e9be52f} \\
  Opens key:
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprocserverx86
  Opens key:
                                  HKCR\clsid\\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\\{inprocserverx86}
  Opens key:
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\localserver32
                                  HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\localserver32
  Opens key:
  Opens key
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprochandler32
  Opens key:
                                  HKCR \verb|\clsid|{eb082ba1-df8a-46be-82f3-35bf9e9be52f} \verb|\inprochandler32| \\
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
  Opens key:
35bf9e9be52f}\inprochandlerx86
                                  HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\inprochandlerx86
  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\localserver
  Opens key:
                                  HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\localserver
  Opens key:
                                  HKLM\system\currentcontrolset\services\napagent\qecs\79617
  Opens key:
                                  HKLM\system\currentcontrolset\services\napagent\gecs\79618
  Opens key:
                                   HKLM\system\currentcontrolset\services\napagent\qecs\79619
  Opens key:
                                  HKLM\system\currentcontrolset\services\napagent\qecs\79620
  Opens key:
                                   HKLM \ system \ current control set \ services \ napagent \ qecs \ \ 79621
  Opens key:
                                   HKLM\system\currentcontrolset\services\napagent\qecs\79623
  Opens kev:
                                  HKLM\system\currentcontrolset\services\napagent\localconfig\gecs\79617
                                   HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79618
  Opens key:
```

HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79619

Opens key:

```
Opens key:
                                   HKLM \ system \ current controls et \ services \ napagent \ local config \ qecs \ \ 79620
  Opens key:
                                   HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79621
  Opens key:
                                   HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79623
  Opens kev:
                                   HKCU\software\classes\appid\netsh.exe
  Opens key:
                                   HKCR\appid\netsh.exe
  Opens key:
                                   HKLM\software\microsoft\hcs
  Opens key:
                                   HKCU \setminus software \setminus classes \setminus clsid \setminus \{8bc3f05e-d86b-11d0-a075-00c04fb68820\}
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\treatas
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
                                   Opens key:
                                   HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
  Opens key:
00c04fb68820}\inprocserverx86
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86
  Opens key:
  Opens key
                                   HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\localserver32
  Opens key:
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32
  Opens key:
                                   HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\inprochandler32
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandlerx86
  Opens key:
                                   HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
  Opens key:
00c04fb68820}\localserver
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
  Opens key:
  Opens key:
                                   HKCU\software\classes\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:
                                   HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
                                   HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
  Opens key:
  Opens kev:
                                   HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
  Opens key:
                                   HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
  Opens key:
                                   HKCR \verb|\| f309ad18-d86a-11d0-a075-00c04fb68820| \verb|\| proxystubclsid32| \\
  Opens key:
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:
                                   HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
  Opens key:
00aa004b2e24}\treatas
  Opens key:
                                   HKCR \ clsid \ \{7c857801-7381-11cf-884d-00aa004b2e24\} \ treat as
  Opens key
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
  Opens key:
                                   HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
  Opens key:
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserverx86
                                   HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\localserver32
  Opens key:
                                   HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
  Opens key:
00aa004b2e24}\inprochandler32
  Opens key:
                                   \label{lem:hkcrclsid} $$HKCR\clsid_{7c857801-7381-11cf-884d-00aa004b2e24}\in All $$\clsid_{7c857801-7381-11cf-884d-00aa004b2e24}$$
  Opens key:
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandlerx86
  Opens key:
                                   HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86
  Opens key:
                                   HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\localserver
  Opens key:
                                   Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemsvc.dll
  Opens key:
                                   HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
  Opens kev:
                                   HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
                                   HKCU \setminus software \setminus classes \setminus interface \setminus \{d4781cd6 - e5d3 - 44df - ad94 - e5d3 - e5d3
  Opens key:
930efe48a887}\proxystubclsid32
  Opens key:
                                   HKCR\interface { d4781cd6-e5d3-44df-ad94-930efe48a887 } \proxystubclsid32 \\
                                   HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
  Opens key:
  Opens key:
                                   HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
                                   HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-
  Opens key:
00aa003240c7}\proxystubclsid32
  Opens key:
                                   Opens key:
                                   HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\treatas
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
  Opens key:
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\ \ inprocserver 32
                                   HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
  Opens key:
ce99a996d9ea}\inprocserverx86
  Opens key:
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprocserverx86
  Opens key:
                                   HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\localserver32
  Opens key:
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32
                                   HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
  Opens kev
```

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32

ce99a996d9ea}\inprochandler32

```
HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
Opens key:
```

ce99a996d9ea}\inprochandlerx86 Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86

Opens kev: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\localserver

Opens key: $HKCR \clsid \d68af00a-29cb-43fa-8504-ce99a996d9ea \localserver$

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

options\ntdsapi.dll

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

options\fastprox.dll

Opens key:

 $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ ni \ 6faf58 \ 19ab8d57 \ ni \ native images in dex \ v2.0.50727_32 \ ni \ native images in dex \ native images \ native images in dex \ native images \ native$

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 6faf58 \ 19ab8d57 \ 12ab2 \ new \ 12ab2 \ 12ab2 \ new \ 12$

Opens key:

Opens key:

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-00000000001} Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-

00000000001}\proxystubclsid32

HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32 Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} Opens key:

 $HKCR \verb|\clsid| \{1b1cad8c-2dab-11d2-b604-00104b703efd\}$ Opens key: Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\treatas

Opens key: $HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas$ HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-Opens key:

00104b703efd}\inprocserver32

 $HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32$ Opens key:

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserverx86

 $HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86$ Opens key:

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32

Opens key HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler32

Opens key: $HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32$

HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-Opens key:

00104b703efd}\inprochandlerx86

Opens key: $HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\ \ inprochandler x86$

Opens key HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver

HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd} Opens key:

HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd} Opens key: Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-

00104b703efd}\proxystubclsid32

Opens key: $HKCR\ interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \ \ proxystubclsid32$ Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-00104b703efd}

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd} Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-

00104b703efd}\proxystubclsid32

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\system.configuration.ni.dll

Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\system.xml.ni.dll

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

options\hnetcfg.dll

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

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens kev: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$

options\wshtcpip.dll

Opens key: HKLM\system\currentcontrolset\services\.net clr networking\performance HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4} Opens key:

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4} HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-Opens kev:

b913c40c9cd4}\treatas

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserver32

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32 Opens key: Opens key:

HKCU\software\classes\clsid\{304ce942-6e39-40d8-943ab913c40c9cd4}\inprocserverx86

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserverx86

HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a Opens key:

b913c40c9cd4}\localserver32

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprochandler32

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32

Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprochandlerx86

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandlerx86 Opens kev:

HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\localserver

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\localserver Opens key: $HKLM \system \current controls et \services \shared access \parameters \firewall policy \standard profile \authorized applications \list$ Opens key: HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2} Opens key: HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2} Opens key: HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\treatas Opens key: HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\treatas HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-Opens key: 6acb603462d2}\inprocserver32 Opens key: HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprocserver32 Opens key: HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprocserverx86 Opens key: $\label{lem:hkcr} $$ HKCR\clsid\\{ec9846b3-2762-4a6b-a214-6acb603462d2}\\ inprocserverx86$ Opens key: HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\localserver32 HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\localserver32 Opens key: Opens key: HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprochandler32 Opens key: HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-Opens key: 6acb603462d2}\inprochandlerx86 Opens key: HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprochandlerx86 Opens key: c7d49d7cecdc} Opens kev HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\localserver Opens key: HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\localserver Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll Opens key: HKLM\software\policies\microsoft\cryptography Opens kev: HKLM\software\microsoft\crvptographv HKLM\software\microsoft\cryptography\offload Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: $\label{lem:hklm} \verb+Kklm\+ software\+ windows nt\+ current version\+ winlogon [leaktrack]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mscoree.dll[checkapphelp] HKLM\system\currentcontrolset\control\session Queries value: manager\appcompatibility[disableappcompat] Queries value: HKLM\software\microsoft\.netframework[installroot] Queries value: HKLM\software\microsoft\.netframework[clrloadlogdir] Queries value: HKLM\software\microsoft\.netframework[onlyuselatestclr] Oueries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\microsoft\windows Queries value: $\verb|nt\currentversion\compatibility32[0fe92a59448dcd7b0d7f239c237a351e]|$ Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[0fe92a59448dcd7b0d7f239c237a351e] Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls] HKCU\control panel\desktop[multiuilanguageid] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mscorwks.dll[checkapphelp] Queries value: HKLM\software\microsoft\.netframework[gcstressstart] HKLM\software\microsoft\.netframework[gcstressstartatjit] Queries value: HKLM\software\microsoft\.netframework[disableconfigcache] Oueries value: Queries value: HKLM\software\microsoft\fusion[cachelocation] Oueries value: HKLM\software\microsoft\fusion[downloadcachequotainkb] Oueries value: HKLM\software\microsoft\fusion[enablelog] Queries value: HKLM\software\microsoft\fusion[logginglevel] HKLM\software\microsoft\fusion[forcelog] Queries value: Queries value: HKLM\software\microsoft\fusion[logfailures] Queries value: HKLM\software\microsoft\fusion[versioninglog] Oueries value: HKLM\software\microsoft\fusion[logresourcebinds] Oueries value: HKLM\software\microsoft\fusion[uselegacyidentityformat] Oueries value: HKLM\software\microsoft\fusion[disablemsipeek] HKLM\software\microsoft\fusion[noclientchecks] Queries value: Queries value: HKLM\system\setup[systemsetupinprogress] HKCU\control panel\desktop[smoothscroll] Queries value: Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 [latest index]$ Oueries value: $HKLM \verb|\software\microsoft| fusion \verb|\nativeimagesindex| v2.0.50727_32 \verb|\index9c[niusagemask]| \\$ Oueries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus index 9c[ilus agemask]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 8[display name]$

 $HKLM \ software \ |\ microsoft \ fusion \ |\ magesindex \ |\ v2.0.50727_32 \ |\ mildown \ \ |\ mildown \ |\$

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[configstring] Queries value: $HKLM \ software \ |\ microsoft \ fusion \ fusion \ |\ microsoft \ fusion \ f$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 8[evalation data]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i \setminus 181938c6 \setminus 7950e2c5 \setminus 8[status]$ Queries value: $HKLM \ software \ `microsoft \ fusion \ native images index \ v2.0.50727_32 \ iildependencies]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 8[nidependencies]$ HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[missingdependencies] Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[displayname] Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 7950e2c5 \ 3838a3a4 \ 8[status]$ $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 7950e2c5 \ 3838a3a4 \ [modules]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\il\7950e2c5\3838a3a4\8[sig] Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 7950e2c5 \setminus 3838a3a4 \setminus 8[last modtime]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[mscorlib, 2.0.0.0, , b77a5c561934e089, x86]$ Oueries value: HKLM\svstem\currentcontrolset\control\session manager[criticalsectiontimeout] Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout] Queries value: HKCR\interface[interfacehelperdisableall] HKCR\interface[interfacehelperdisableallforole32] Queries value: Oueries value: HKCR\interface[interfacehelperdisabletypelib] HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableall1 Queries value: HKCR\interface\{00020400-0000-0000-c000-00000000046}[interfacehelperdisableallforole32] Queries value: HKLM\software\microsoft\ctf\systemshared[cuas] Queries value: HKCU\keyboard layout\toggle[language hotkey] Oueries value: HKCU\keyboard layout\toggle[hotkey] ${\tt HKCU\keyboard\ layout\toggle[layout\ hotkey]}$ Oueries value: Queries value: HKLM\software\microsoft\ctf[enableanchorcontext] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache] HKLM\software\microsoft\fusion\publisherpolicy\default[latest] Queries value: Oueries value: HKLM\software\microsoft\fusion\publisherpolicy\default[index1] Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default[legacypolicy timestamp]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus ni \setminus 1c22df2f \setminus 4f99a7c9 \setminus 3f[displayname]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus ni \setminus 1c22df2f \setminus 4f99a7c9 \setminus 3f[configmask]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 1c22df2f \ 4f99a7c9 \ 3f[configstring]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[mvid] Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 1c22 df2f \ 4f99a7c9 \ 3f[evalation data]$ Queries value: Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus ni \setminus 1c22df2f \setminus 4f99a7c9 \setminus 3f[ildependencies]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[nidependencies] Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 1c22 df2f \ 4f99a7c9 \ 3f[missing dependencies]$ $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus c991064 \setminus 3880e29a \setminus 1d[displayname]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus c991064 \setminus 3880e29a \setminus 1d[status]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ c991064 \ 3880e29a \ 1d[modules]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ c991064 \ 3880e29a \ ld [last mod time]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 6dc7d4c0\ 7cd935b4 \ e[displayname]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 6dc7d4c0 \setminus 7cd935b4 \setminus e[status]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 6dc7d4c0\ 7cd935b4 \ e[modules]$ Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ i1 \ 6dc7d4c0 \ 7cd935b4 \ [sig]$

Oueries value:

Queries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 6dc7d4c0\ 7cd935b4 \ e[last mod time]$

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5\ 32e43dd1\ d[displayname]$

```
\label{lem:hklmsoftware} HKLM \software \end{area} HKLM \software \end{area} IN $$ Oueries value:
```

 $\label{lem:hklmsoftware} HkLM \software \microsoft \subseteq in a tive images in dex \subseteq 2.0.50727_32 \subseteq 13 \subseteq 2.0.50727_32 \subseteq 13 \subseteq 2.0.50727_32 \subseteq 13 \subseteq 2.0.50727_32 \subseteq 2$

 $\label{lem:hklmsoftware} HKLM \software \since \s$

 $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ il\ 3ced59c5\ 32e43dd1\ d[last mod time] \\ Oueries\ value:$

 $\label{lem:hklmsoftware} HkLM \software \sin dex \v2.0.50727_32 \sin f6e8397 \sin dex \v2.0.50727_32 \sin f6e8397 \sin dex \sin$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\f6e8397\9edd04c\4e[status]
Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \since \s$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[lastmodtime]
Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \since \s$

 $\label{local-prop} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl v2.0.50727_32\mbox{\sl}\sl 2b1a4e4\502472a2\3e[status]\ Queries\ value:$

 $\label{local-operator} HKLM \software \mbox{\le index$} 2.0.50727_32 \mbox{$\le$ index$} 2.0.50727_32 \mbox{$\le$ index$} Queries value:$

 $\label{lem:hklmsoftware} HKLM \software \microsoft \size 1.0.50727_32 \il\2b1a4e4 \size 2.3e[sig] Queries value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\502472a2\3e[lastmodtime]
Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\le index$} \scales \s$

 $\label{lem:hklmsoftware} HkLM \software \end{area} Hklm \software \end{area} Nucries \ value \end{area} Oueries \ value \end{area} V2.0.50727_32 \end{area} il \area \end{area} V2.0.50727_32 \end{area} in \area \end{area} V2.0.50727_32 \end{area} in \area \end{area} V2.0.50727_32 \end{area} in \area \end{area} V2.0.50727_32 \end{area} V2.$

 $\label{thm:hklm} \begin{tabular}{lll} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\slass\cite{Linear} 1.24bf93f6\129642c9\22\[sig] Queries\ value: \end{tabular}$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\129642c9\22[lastmodtime]
 Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \il\4f99a7c9 \340b8570 \4f[status] \\ Queries value:$

 $\label{local-observation} HKLM \software \mbox{$\$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\4f99a7c9\340b8570\4f[sig]
Oueries value:

 $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_32\il\4f99a7c9\340b8570\4f[lastmodtime] \\ Queries\ value:$

 $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ ni\ 30bc7c4f\ 3f50fe4f\ 7[display name] \ Oueries\ value:$

 $\label{lem:hklm} HKLM \software \microsoft \sion \native images in dex \v2.0.50727_32 \ni\30bc7c4f\3f50fe4f\7[configmask] Queries value:$

 $\label{lem:hklmsoftware} HKLM \software \since \s$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[mvid]
Oueries value:

 $\label{local-observable} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727_32\mbox{\sl ni}\sl 30bc7c4f\sl 50fe4f\sl\ 7[evalationdata] \\ Oueries\ value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[status]
Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} in \adiabeta. $0.50727_32 \in \mathbb{N}$ is a partial of the proposed of the p$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[nidependencies]
Queries value:

 $\label{lem:hklmsoftware} HKLM\software\mbox{\colored} wicrosoft\fusion\native\mbox{\colored} mages index\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[missing dependencies] Queries value:$

 $\label{lem:hklmsoftware} HKLM \software \since \s$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[status]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[modules]

 $\label{local-bound} HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[modules] Queries\ value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[sig]
Oueries value:

 $\label{lem:hkim} $$HKIM\software\microsoft\fusion\native images in dex \v2.0.50727_32\il\424bd4d8\2bfe65de\5[last mod time] $$Oueries value:$

 $\label{local-bound} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_32\label{local-bound} 32\label{local-bound} All the continuous continuous local bounds of the contin$

 $\label{local-equation} HKLM \software \mbox{\le index$ \le 0.50727_32$ il \19ab8d57\61dc497f\6[status] Oueries value: }$

 $\label{local-prop} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \il\19 ab 8d 57 \61d c 497f \6[modules] \\ Queries \value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[sig]
Queries value:

 $\label{local-prop} HKLM\software\microsoft\fusion\native\microsoft\subseteq 2.0.50727_32\label{local-prop} All the control of the control o$

```
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[status]
Oueries value:
```

 $\label{local-bound} HKLM\software\microsoft\fusion\native images in dex $$v2.0.50727_32\il\3f50fe4f\7540f5be\7[sig] Oueries value:$

 $\label{thm:hklm} \begin{tabular}{ll} HKLM\software\microsoft\fusion\native images in dex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[last mod time] \\ Oueries\ value: \begin{tabular}{ll} \begi$

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} With \label{lem:hklm$

HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
Oueries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
Oueries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
Oueries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[system.web,2.0.0.0,,b03f5f7f11d50a3a,x86]
Oueries value:

 $HKLM \label{lem:management} HKLM \label{lem:management} HKLM \label{lem:management} HKLM \label{lem:management} Signification \label{lem:management} With \label{lem:man$

HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.remoting,2.0.0.0,,b77a5c561934e089,msil]
Queries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[system.deployment,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} With \label{lem:hklm} HKLM \label{lem:hklm} With \label{lklm} With \labe$

HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[displayname]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configmask]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configstring] Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\2.0.50727_32 \mbox{\mathbb{N} is 161e7e666 \c991064 \13 [mvid] $$ Queries value: $$\colored{ \subseted} $$$

 $\label{local-observation} HKLM \software \mbox{\le 13[evalation data]} \\ Queries \ value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[status]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[ildependencies]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[nidependencies]
 Queries value:

 $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ ni \ 61e7e666 \ c991064 \ 13 \ [missing dependencies] \ Oueries \ value:$

 $\label{lem:hklm} HKLM \software \mbox{$\mbox{$\mathbb{N}$} irrosoft \subseted in a tive images in dex $\mbox{$\mathbb{N}$} 2.0.50727_32 \subseted in \subseted$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[status]
Oueries value:

 $\label{local-prop} HKLM\software\microsoft\fusion\native images index $$ v2.0.50727_32\il\475dce40\3856a4e\10[modules] Oueries\ value:$

 $\label{local-equation} HKLM \software \since \sin$

 $\label{local-operator} HKLM\software\mbox{$\mbox{}\mbox{$

 $\label{local-prop} HKLM \software \mbox{\mathbb{N} icrosoft fusion $$ native images index \scales $$ 2.0.50727_32 il \scales \scales $$ 2d \scales \scal$

 $\label{thm:local-substitute} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \cilv2dd6 ac 50 \cilv1bd3 c34 \cilv30 \c$

 $\label{local-equation} HKLM \software \mbox{$\mbox{$\mathbb{N}$} $ ware \mbox{\mathbb{N}} $ ware \mbo$

 $\label{thm:local-prop} HKLM \software \mbox{\sim1.50727_32\il\2dd6ac50\11bd3c34\30[sig] Queries value:}$

 $\label{local-equation} HKLM \software \mbox{$\mbox{$\mbox{\sim}}$ il \added ac 50 \norm{$\mbox{$\sim$}} 11bd3c34 \added ac 50 \norm{$\mbox{$\sim$}} 12dd6ac 50 \norm{$\mbox{\sim}} 11bd3c34 \added ac 50 \norm{$\mbox{$\sim$}} 12dd6ac 50 \norm{$\mbox{\sim}} 11bd3c34 \added ac 50 \norm{$\mbox{$\sim$}} 12dd6ac 50 \norm{$\mb$

 $\label{thm:local_thm:loc$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\41c04c7e\286a445d\24[status]
Oueries value:

 $\label{local-prop} HKLM \software \microsoft \sion \native images in dex \sindex \sindex \sion \native images in dex \sion \$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[sig]
Oueries value:

 $\label{lem:hklm} $HKLM \setminus software \ensuremath{\mbox{\mbox{\times}} 11\41c04c7e\286a445d\24[last mod time] $$Oueries value$$. $$ value$$$$

 $\label{localization} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[displayname] Queries value:$

 $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ ni\ 3cca06a0\ 6dc7d4c0\ 17[configmask] \ Oueries\ value:$

 $\label{lem:hklmlsoftware} HKLM\software\microsoft\fusion\native\miggesindex\v2.0.50727_32\mi\acca06a0\6dc7d4c0\17\[configstring]\ Queries\ value:$

 $\label{localization} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \ni\3cca06a0\6dc7d4c0\17 \mbox{[mvid]} Oueries value:$

 $\label{localized} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_32\ni\acca06a0\6dc7d4c0\17[evalation data] Queries value:$

 $\label{localization} HKLM \software \mbox{$\mbox{$\mathbb{N}$} irrosoft \subseted in a tive images in dex $$\mbox{\mathbb{N}} 2.0.50727_32 \mbox{\mathbb{N}} irrosoft \subseted in a tive images in dex \subseted in a tive image sindex \subseted$

```
HKLM \label{lem:hklm} Software \mbox{\sca06a0\6dc7d4c0\17[ildependencies]} \\
    Oueries value:
Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 17[missing dependencies]
    Queries value:
Queries value:
HKLM \label{lem:hklm} In the large of the 
    Oueries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} with the label{lem:hklm} With the label{lem:hklm} Software \label{lem:hklm} With the label{lem:hklm} Software \label{lem:hklm} With the label{lem:hkklm} With the
                                                            HKCU\software\5cd8f17f4086744065eb0992a09e05a2[us]
    Queries value:
    Oueries value:
                                                            HKCU\environment[see mask nozonechecks]
    Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
                                                            HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
    Queries value:
    Oueries value:
                                                            HKLM\software\microsoft\rpc[maxrpcsize]
    Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ policies \ \ explorer [no properties my computer]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Queries value:
                                                            \label{local-condition} $HKCR\clsid{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] $$
                                                            HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
    Oueries value:
409d6c4515e9}[drivemask]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
                                                            HKCR\.exe[]
    Queries value:
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                                                            HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Oueries value:
    Oueries value:
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Queries value:
\label{thm:local_continuous} HKCU \software \mbox{\tt microsoft} \windows \scalebox{\tt current} version \scalebox{\tt policies} \scalebox{\tt explorer} \cite{\tt classicshell} \cite{\tt policies} \scalebox{\tt microsoft} \scalebox{\tt microso
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Queries value:
Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Oueries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [hidefileext] \end{tabular}
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
    Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [hideicons]} \end{tabular}
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                                            HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
    Oueries value:
    Oueries value:
HKCU \ software \ `microsoft \ windows \ `current version \ `explorer \ advanced [show superhidden]
\label{thm:linear} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| [separate process] \end{tabular}
    Queries value:
Oueries value:
                                                            HKCR\exefile[docobject]
    Queries value:
                                                            HKCR\exefile[browseinplace]
                                                            HKCR\exefile[isshortcut]
    Queries value:
    Queries value:
                                                            HKCR\exefile[alwaysshowext]
    Queries value:
                                                            HKCR\exefile[nevershowext]
    Oueries value:
                                                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
    Oueries value:
                                                            HKLM\system\wpa\pnp[seed]
```

Queries value:

Queries value:

Oueries value:

Oueries value:

HKLM\system\setup[osloaderpath]

HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]

HKLM\system\setup[systempartition]

HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

```
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
                                    HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion[devicepath]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\setup[loglevel]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\setup[logpath]
  Queries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
  Oueries value:
11e3-9fc7-806d6172696f}[generation]
                                    HKCR\directory[docobject]
  Queries value:
  Oueries value:
                                    HKCR\directory[browseinplace]
  Oueries value:
                                    HKCR\directory[isshortcut]
  Oueries value:
                                    HKCR\directory[alwaysshowext]
  Queries value:
                                    HKCR\directory[nevershowext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
                                    \label{lem:hklmsoftware} \begin{tabular}{l} HKLM \begin{tabular}{l} Software \begin{tabular}{l} Microsoft \begin{tabular}{l} Windows \begin{tabular}{l} Current version \begin{tabular}{l} Version \begin{tabular}{l} Current \begin{tabular}{l} Version \begin{tabular}{l} Current \begin{tabular}{l} Version \begin{tabular}{l} Current \begin{tabula
  Oueries value:
folders[common documents]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
                                    HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
  Oueries value:
  Oueries value:
                                    HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
  Queries value:
                                    HKCR\.asp[]
  Oueries value:
                                    HKCR\.bat[]
  Oueries value:
                                    HKCR\.cer[]
                                    HKCR\.chm[]
  Oueries value:
  Queries value:
                                    HKCR\.cmd[]
  Queries value:
                                    HKCR\.com[]
  Queries value:
                                    HKCR\.cpl[]
  Queries value:
                                    HKCR\.crt[]
                                    HKLM\software\microsoft\com3[com+enabled]
  Oueries value:
                                    HKLM\software\microsoft\ole\minimumfreemempercentagetocreateprocess1
  Oueries value:
  Queries value:
                                    {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create object]}
  Queries value:
                                    HKLM\software\microsoft\com3[regdbversion]
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
  Queries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
  Oueries value:
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                                    HKLM\software\microsoft\internet
  Queries value:
explorer \verb|\main\featurecontrol\feature_protocol_lockdown[0fe92a59448dcd7b0d7f239c237a351e.exe]|
  Queries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
                                    HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Oueries value:
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablepunycode]
  Queries value:
                                    HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
  Queries value:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[0fe92a59448dcd7b0d7f239c237a351e.exe]
                                    HKCU\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature localmachine lockdown[*]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[0fe92a59448dcd7b0d7f239c237a351e.exe]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[specialfolderscachesize]
```

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cookies]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\zones\0[1806]

Oueries value: HKCR\exefile\shell[1

Queries value: HKCR\exefile\shell\open\command[] HKCR\exefile\shell\open\command[command] Queries value:

Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid]

Queries value:

HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\trojan.exe] Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]|$

HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]

HKLM\system\wpa\mediacenter[installed] Queries value:

Oueries value:

 $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]|$

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

be2efd2c1a33}[itemdata]

Oueries value:

be2efd2c1a33}[saferflags]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemdata]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-4666f-9b89-46666f-9b89-4666$ edd5fbde1328}[hashalg]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemsize]

Oueries value:

edd5fbde1328}[saferflags]

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57$ b813f72dbb91}[itemdata]

Queries value:

b813f72dbb91}[hashalg]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[itemsize]

Queries value:

b813f72dbb91}[saferflags]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16$ 7c29ddecae3f}[itemdata] Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16$ 7c29ddecae3f}[itemsize]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16$ 7c29ddecae3f}[saferflags]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemdata]

Oueries value:

085bcc18a68d}[hashalg]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsize]

Oueries value:

085bcc18a68d}[saferflags]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[itemdata]

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc}[hashalg]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[itemsize]

```
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe
b91490411bfc}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
                                            HKCU\software\microsoft\windows\currentversion\explorer\shell
   Queries value:
folders[cache]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
   Oueries value:
                                           HKLM\software\microsoft\windows
nt\currentversion\compatibility32[trojan]
                                            HKLM\software\microsoft\windows nt\currentversion\ime
   Oueries value:
compatibility[trojan]
                                            HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:
   Oueries value:
                                            HKLM\software\microsoft\ole[defaultaccesspermission]
                                            HKLM \setminus system \setminus current control \setminus lsa[everyone includes an onymous]
   Oueries value:
   Oueries value:
                                            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:
HKCU\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
                                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[startup]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\compatibility32[netsh]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[netsh]
   Queries value:
                                            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Queries value:
                                            HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 1]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
   Queries value:
                                            HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 7]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
   Oueries value:
                                            HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi1]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi51
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
   Oueries value:
                                            HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi7]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
   Oueries value:
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
   Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
   Oueries value:
   Oueries value:
                                            HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 2]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
   Queries value:
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
   Queries value:
Queries value:
HKLM \verb|\software\microsoft| windows \verb|\currentversion| telephony [tapi32 requestre trytime out] \\
   Oueries value:
                                            HKCU\software\microsoft\multimedia\audio[systemformats]
   Oueries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
   Oueries value:
HKLM \ software \ microsoft \ audiocompression manager \ driver cache \ msacm. im a adpcm [cformattags] \ driver \ cache \ msacm. im a adpcm \ msacm \ msacm
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
   Oueries value:
HKLM\software\microsoft\windows
   Oueries value:
```

nt\currentversion\drivers32[msacm.msadpcm]

Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport] Queries value: $HKLM \verb|\software\microsoft\audiocompression| manager \verb|\driver| cache \verb|\msadpcm[cformattags]| and the software \verb|\msadpcm[cformattags]| and the software$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg711] Oueries value: Queries value: Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msg711[cfilter tags]$ HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.msgsm610] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport] Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msgsm610[cformattags]$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache] Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msgsm610[cfilter tags]$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.trspch] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags] Queries value: $HKLM \label{lem:hklm} \\ KLM \label{lem:hklm} HKLM \label{lem:hklm} \\ Software \label{lem:hklm} \\ icrosoft \label{lem:hklm} \\ and icrosoft \label{lem:hklm} \\$ Queries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.trspch[cfiltertags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msg723] Oueries value: $HKLM \verb|\software\microsoft\audiocompression manager\driver cache \verb|\msacm.msg723[fdwsupport]| \\$ $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msg723[cformattags]$ Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache] Oueries value: $HKLM \verb|\software\microsoft| audio compression manager \verb|\driver| cache \verb|\msacm.msg723| [cfilter tags]|$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags] Oueries value: $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msaudio1[aformattagcache]$ Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl_anet] Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. sl_anet[fdwsupport]$ Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags] Queries value: $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. sl_anet[aformattagcache]$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cfiltertags] HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] Oueries value: Oueries value: Queries value: $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} which is a constant and in the lemma substitution of the le$ Queries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ mac m. iac 2 [a formattag cache]$ Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.iac2[cfilter tags]$ HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.13acm] Queries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[fdwsupport] Oueries value: $HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox| 13acm[cformattags]$ Queries value: $HKLM \verb|\software\microsoft\audiocompression manager\driver cache\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\software\mbox{|} msacm. 13 acm [a formattag cache] and the software \verb|\$

 $\label{lem:hklmsoftware} HKLM\software\microsoft\audiocompression manager\drivercache\msacm.13acm[cfiltertags] \\ Queries\value: HKCU\software\microsoft\multimedia\audio\compression \\ manager\msacm[nopcmconverter]$

Queries value: HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00[priority1] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel] Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[chkaccdebuglevel] HKLM\system\currentcontrolset\control\productoptions[producttype] Queries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local settings] HKLM\software\microsoft\windows Oueries value: nt\currentversion\winlogon[rsopdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Oueries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing] Queries value: HKCU\control panel\desktop[lamebuttontext] Queries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters [winsock_registry_version]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ [next_catalog_entry_id]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries] Queries value: Queries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000002 \ [packed catalog item]$ Oueries value: Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000004 \ [packed catalog item]$ Queries value: Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000008[packedcatalogitem] Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000009 \ [packed catalog item]$ Queries value: $HKLM \ system \ \ current controls et \ services \ \ winsock 2 \ parameters \ protocol_catalog \ \ catalog_entries \ \ 0000000000010 \ [packed catalog item]$ Queries value: Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries] Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000001[library path]$ Queries value: 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: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000001[version] Oueries value: Queries value: Queries value: Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog5 \ catalog_entries \ 0000000000002 \ [providerid]$ Oueries value: $HKLM \ system \ current controls et \ services \ win sock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 0000000000002 \ [address family]$ Queries value: $HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 0000000000002 \ [supported names pace]$ Oueries value: Oueries value: $HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000002 \ [version]$ Queries value: Oueries value: Queries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 1000000000003 \ [displaystring]$ Queries value: $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ namespace_catalog5 \ \ catalog_entries \ \ \ 000000000003 \ [providerid]$

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 000000000003 \ [address family]$

Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000003 [supported namespace]$ Queries value:

 $HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ namespace_catalog5 \ \ catalog_entries \ \ 000000000003 \ [enabled]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version] Queries value:

Queries value:

HKLM\svstem\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value:

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

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

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]

Oueries value:

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

Queries value:

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

Oueries value:

Oueries value:

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

Queries 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[filterclusterip]

Queries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value:

Oueries value:

 $\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+dns \ cache \ \verb+parameters \ [query ipm atching]$

HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value:

Queries value:

 $HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[registration enabled]|$

Oueries 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]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]

Oueries value:

HKLM\svstem\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]

Oueries value:

Queries value:

Oueries value:

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

Oueries value:

Queries value:

Queries value:

Oueries 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]

Oueries value:

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

Oueries value:

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

Queries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]

Queries value:

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

Oueries value:

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

```
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
    Queries value:
                                                         HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
    Oueries value:
                                                          HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-00000000000001
    Oueries value:
                                                         HKLM\software\microsoft\windows nt\currentversion[currentbuildnumber]
                                                          HKLM\software\microsoft\wbem\cimom[logging]
    Queries value:
    Queries value:
                                                         HKLM\software\microsoft\wbem\cimom[logging directory]
                                                         \label{localization} \mbox{HKLM\software\mbox{\sc microsoft\wbem\cimom[log file max size]}}
    Queries value:
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-
    Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
    Queries value:
    Queries value:
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
    Queries value:
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel1
                                                         HKLM\software\microsoft\wbem\cimom[repository directory]
    Oueries value:
    Oueries value:
                                                         HKLM\software\microsoft\tracing[enableconsoletracing]
    Queries value:
                                                         HKLM\software\microsoft\tracing\fwcfg[enablefiletracing]
                                                          HKLM\software\microsoft\tracing\fwcfg[filetracingmask]
    Queries value:
    Oueries value:
                                                          HKLM\software\microsoft\tracing\fwcfg[enableconsoletracing]
    Oueries value:
                                                         HKLM\software\microsoft\tracing\fwcfg[consoletracingmask]
    Queries value:
                                                         HKLM\software\microsoft\tracing\fwcfg[maxfilesize]
    Queries value:
                                                         HKLM\software\microsoft\tracing\fwcfg[filedirectory]
    Queries value:
                                                         HKLM \label{lem:hcm} \label{lem:hcm} HKLM \label{lem:hcm} In the lem \label{lem:hcm} With \label{lem:hcm} HKLM \label{lem:hcm} \label{lem:hcm} \label{lem:hcm} \label{lem:hcm} HKLM \label{lem:hcm} \label{lcm} \labell} \label{lcm} \label{lcm} \labell} \label{lcm} \labell{lcm} \labell{lcm} \labell} \labell{lcm} \labell{lcm} \labell{lcm} \labell} \labell{lcm} \labell{lcm} \labell{lcm} \labell} \labell{lcm
card csp v1.0[type]
   Queries value:
                                                         HKLM\software\microsoft\cryptography\defaults\provider\infineon sicrypt
base smart card csp[type]
                                                         \label{thm:local} \verb+HKLM\software\microsoft\cryptography\defaults\provider\microsoft\ base
    Oueries value:
cryptographic provider v1.0[type]
                                                         \label{lem:hklm} \mbox{HKLM\software\mbox{$\mbox{$\mbox{microsoft}$ cryptography\defaults\provider\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$
    Queries value:
dss and diffie-hellman cryptographic provider[type]
                                                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
   Queries value:
dss cryptographic provider[type]
    Queries value:
                                                         HKLM \setminus software \setminus icrosoft \setminus cryptography \setminus defaults \setminus provider \setminus microsoft \ dh
schannel cryptographic provider[type]
    Queries value:
                                                         enhanced cryptographic provider v1.0[type]
                                                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft
   Queries value:
enhanced dss and diffie-hellman cryptographic provider[type]
    Queries value:
                                                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced rsa and aes cryptographic provider (prototype)[type]
    Queries value:
                                                         HKLM \verb|\software\microsoft\cryptography\defaults\provider\microsoft\ rsa
schannel cryptographic provider[type]
                                                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
    Oueries value:
cryptographic provider[type]
                                                         Queries value:
cryptographic service provider[type]
                                                         HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
    Queries value:
28ecbd96ba8c}\inprocserver32[inprocserver32]
                                                         HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprocserver32[]
    Queries value:
                                                         HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}[appid]
    Oueries value:
    Oueries value:
                                                         HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprocserver32[threadingmodel]
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[displayname]
    Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus ni \setminus 159a66b8 \setminus 424bd4d8 \setminus 2a[configmask]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 159a66b8 \ 424bd4d8 \ 2a[configstring]
\label{local-hamilton} HKLM \software \microsoft \fusion \native images index \normalfallow 2.0.50727\_32 \ni \normalfallow 4.44bd4d8 \normalfallow 2.0.50727\_32 \ni \normalfallow 2.0.50
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 159a66b8 \ 424bd4d8 \ 2a[evalation data]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 159a66b8 \ 424bd4d8 \ 2a[status]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 159a66b8 \setminus 424bd4d8 \setminus 2a[ildependencies]
    Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 159a66b8 \ 424bd4d8 \ 2a[nidependencies]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i159a66b8 \setminus 424bd4d8 \setminus 2a[missing dependencies]
    Queries value:
                                                         {\tt HKLM \ } system \verb|\ current controlset \ \\ services \verb|\ napagent \verb|\ local config[enable|]| \\
tracing]
   Oueries value:
                                                         HKLM\system\currentcontrolset\services\napagent\localconfig[tracing
level1
                                                         HKCR\clsid\{eb082ba1-df8a-46be-82f3-
    Queries value:
```

```
35bf9e9be52f}\inprocserver32[inprocserver32]
                                          HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\inprocserver32[]
  Oueries value:
   Queries value:
                                          HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}[appid]
  Queries value:
                                          HKCR\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprocserver32[threadingmodel]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[friendly
name]
   Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[description]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[version]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[enabled]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[vendor name]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[info clsid]
   Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[config clsid]
   Queries value:
                                          clsid]
  Queries value:
                                          date1
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79617[component
type]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[friendly
name]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[description]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[version]
   Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[enabled]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[vendor name]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[info clsid]
  Queries value:
                                          HKLM\svstem\currentcontrolset\services\napagent\qecs\79618[config clsid]
  Oueries value:
                                          clsid1
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[registration
date1
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79618[component
type]
  Queries value:
                                          HKLM \ system \ current control set \ services \ napagent \ qecs \ 79619 [friendly] \ and \ system \
name]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79619[description]
   Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79619[version]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79619[enabled]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\gecs\79619[vendor name]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79619[info clsid]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79619[config clsid]
  Queries value:
                                          clsid]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79619[registration
date1
  Queries value:
                                          type]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[friendly
name1
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[description]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[version]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[enabled]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[vendor name]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[info clsid]
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[config clsid]
   Oueries value:
  Queries value:
                                          HKLM\svstem\currentcontrolset\services\napagent\gecs\79620[validator
clsid1
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79620[registration
date]
  Queries value:
                                          HKLM \verb|\system| current control set \verb|\services| napagent \verb|\qecs| 79620 [component] | the control set \verb|\system| current control set control s
type]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[friendly
name1
  Oueries value:
                                          HKLM \verb|\system| current controlset \verb|\services| napagent \verb|\qecs| 79621 [description]|
   Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[version]
   Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[enabled]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[vendor name]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[info clsid]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[config clsid]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[validator
clsid1
  Queries value:
                                          date1
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79621[component
type]
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79623[friendly
  Oueries value:
name1
   Queries value:
                                          HKLM \verb|\system| current controlset \verb|\services| napagent \verb|\qecs| 79623 [description]|
   Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79623[version]
  Queries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79623[enabled]
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79623[vendor name]
  Oueries value:
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79623[info clsid]
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79623[config clsid]
   Queries value:
                                          clsid1
  Oueries value:
                                          HKLM\system\currentcontrolset\services\napagent\qecs\79623[registration
date1
  Queries value:
```

```
type]
   Queries value:
HKLM\system\currentcontrolset\services\napagent\localconfig[plumbipsecpolicy]
                                               HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
   Oueries value:
   Oueries value:
                                               HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
   Queries value:
                                               HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
                                               HKCR\interface \{f309ad18-d86a-11d0-a075-00c04fb68820\}\proxystubclsid32[]
   Queries value:
   Queries value:
                                               HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
                                              HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
   Oueries value:
                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
   Oueries value:
   Oueries value:
                                               HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel1
                                               Queries value:
                                               HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
   Queries value:
   Oueries value:
                                              HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
   Oueries value:
                                              HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
                                               HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
   Queries value:
                                              HKCR\clsid\{d68af00a-29cb-43fa-8504-
   Queries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                                              HKLM\software\microsoft\wbem\cimom[processid]
   Oueries value:
   Oueries value:
                                               HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
   Queries value:
                                               HKLM\software\microsoft\wbem\cimom[contextlimit]
   Queries value:
                                               HKLM\software\microsoft\wbem\cimom[objectlimit]
   Queries value:
                                               HKLM\software\microsoft\wbem\cimom[identifierlimit]
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 6faf58 \ 19ab8d57 \ 12[displayname]
   Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[configmask]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 6faf58 \ 19ab8d57 \ 12[configstring]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus hi \setminus faf58 \setminus 19ab8d57 \setminus 12[mvid]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ ni \ 6faf58 \ 19ab8d57 \ 12[evalation data]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 6faf58 \ 19ab8d57 \ 12[status]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 6faf58 \setminus 19ab8d57 \setminus 12[ildependencies]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 6faf58 \ 19ab8d57 \ 12[nidependencies]
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 6faf58 \ 19ab8d57 \ 12[missing dependencies]
   Oueries value:
HKLM \verb|\software| microsoft| fusion \verb|\native| mages index \verb|\v2.0.50727_32 \verb|\il| \ 75638 fee \verb|\78136415 \verb|\2d[displayname]|
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il \ 75638 fee \ 78136415 \ 2d[status]
   Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d[modules]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 75638 fee\ 78136415 \ 2d[sig] \ microsoft \ fusion\ native images index \ v2.0.50727\_32 \ il\ 75638 fee\ 78136415 \ 2d[sig] \ microsoft\ native images index \ v2.0.50727\_32 \ il\ 75638 fee\ 78136415 \ 2d[sig] \ microsoft\ native images index \ v2.0.50727\_32 \ il\ 75638 fee\ 78136415 \ 2d[sig] \ microsoft\ native images index \ native images \ nati
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d[lastmodtime]
   Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.data.sqlxml,2.0.0.0,,b77a5c561934e089,msil]
                                               HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
   Oueries value:
   Oueries value:
                                               HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
                                              HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
   Queries value:
                                               HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
   Oueries value:
                                              HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
   Queries value:
00104b703efd}\inprocserver32[threadingmodel]
   Oueries value:
                                              HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
   Queries value:
                                               HKCR \ | \ HKCR \ | 
                                               HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
   Queries value:
   Queries value:
                                               HKLM\system\currentcontrolset\services\winsock\parameters[transports]
                                               HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Queries value:
   Oueries value:
HKLM \ system \ current control set \ 's ervices \ 'tcpip \ parameters \ 'winsock [minsock addrlength]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
   Queries value:
                                               HKLM\system\currentcontrolset\services\.net clr
networking\performance[library]
                                              HKLM\system\currentcontrolset\services\.net clr
  Queries value:
networking\performance[ismultiinstance]
                                               {\tt HKLM \ } system \verb| current control set \verb| services \verb| .net clr | \\
   Oueries value:
networking\performance[first counter]
   Queries value:
                                              HKLM\system\currentcontrolset\services\.net clr
networking\performance[categoryoptions]
                                               HKLM\system\currentcontrolset\services\.net clr
   Queries value:
networking\performance[filemappingsize]
                                              HKLM\system\currentcontrolset\services\.net clr
   Oueries value:
networking\performance[counter names]
```

HKCR\clsid\{304ce942-6e39-40d8-943a-Queries value: b913c40c9cd4}\inprocserver32[inprocserver32] HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[] Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[appid] Oueries value: Oueries value: HKCR\clsid\{304ce942-6e39-40d8-943ab913c40c9cd4}\inprocserver32[threadingmodel] Queries value: and settings\admin\local settings\temp\trojan.exe] HKCR\clsid\{ec9846b3-2762-4a6b-a214-Oueries value: 6acb603462d2}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprocserver32[] Oueries value: Queries value: HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}[appid] Queries value: c7d49d7cecdc}[enabledhcp] Oueries value: c7d49d7cecdc}[leaseobtainedtime] Queries value: c7d49d7cecdc}[leaseterminatestime] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpserver]

HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

HKCR\clsid\{ec9846b3-2762-4a6b-a214-Oueries value:

6acb603462d2}\inprocserver32[threadingmodel]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[queryadaptername]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[disableadapterdomainname]

Queries value:

c7d49d7cecdc}[registrationenabled]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registeradaptername]

Queries value:

c7d49d7cecdc}[registrationmaxaddresscount]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[maxnumberofaddressestoregister]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[domain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpdomain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[ipautoconfigurationenabled]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[addresstype]

Queries value:

c7d49d7cecdc}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpnameserver]

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

Queries value:

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

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wicrosoft \ strong$ Queries value:

cryptographic provider[image path]

Oueries value: HKLM\software\microsoft\cryptography[machineguid]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]

Sets/Creates value: HKCU\software\5cd8f17f4086744065eb0992a09e05a2[us]

Sets/Creates value: HKCU\environment[see_mask_nozonechecks]

Sets/Creates value:

 $HKCU \ software \ microsoft \ windows \ shell no roam \ muicache \ [c:\ docume-1\ admin\ locals-1\ temp\ trojan.exe]$

Sets/Creates value:

HKCU\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]

Sets/Creates value

HKLM\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]

Sets/Creates value:

and settings\admin\local settings\temp\trojan.exe]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[appdata]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

```
folders[personal]
 Value changes:
806d6172696f}[baseclass]
                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ shell
 Value changes:
folders[common documents]
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
 Value changes:
folders[desktop]
 Value changes:
                          HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common desktop]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\zonemap[uncasintranet]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[startup]
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[logsessionname]
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[active]
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\eappcfg[controlflags]
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier[guid]
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier[bitnames]
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\eappprxy[logsessionname]
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy[active]
  Value changes:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\tracing\microsoft\eappprxy[controlflags]|
                          HKLM\software\microsoft\windows
 Value changes:
\verb| nt\currentversion \verb| tracing \verb| microsoft \verb| eappprxy \verb| trace identifier [guid]|
 Value changes:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\tracing\microsoft\eappprxy\traceidentifier[bitnames]|
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil[logsessionname]
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\qutil[active]
 Value changes:
                          {\tt HKLM \backslash software \backslash microsoft \backslash windows}
\verb| nt\currentversion \verb| tracing \verb| microsoft \verb| qutil[controlflags]| \\
 Value changes:
                          HKLM\software\microsoft\windows
\verb| nt\current version \verb| tracing \verb| microsoft \verb| qutil \verb| trace identifier [guid]| \\
                          HKLM\software\microsoft\windows
 Value changes:
\verb|nt\currentversion\tracing\microsoft\qutil\traceidentifier[bitnames]|
                          HKLM\software\microsoft\windows
 Value changes:
\verb|nt\currentversion\tracing\microsoft\nap\netsh[logsessionname]|\\
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\nap\netsh[active]
                          HKLM\software\microsoft\windows
 Value changes:
\verb|nt\currentversion\tracing\microsoft\nap\netsh[controlflags]|
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh\napmontr[guid]
  Value changes:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\tracing\microsoft\nap\netsh\napmontr[bitnames]|
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\qagent[logsessionname]
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\qagent[active]
 Value changes:
                          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent[controlflags]
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\qagent\traceidentifier[guid]
                          HKLM\software\microsoft\windows
 Value changes:
nt\currentversion\tracing\microsoft\qagent\traceidentifier[bitnames]
```

Value changes:

Value changes:

 $HKLM \ software \ microsoft \ windows \ current version \ [5cd8f17f4086744065eb0992a09e05a2] \ microsoft \ windows \ current version \ microsoft \ windows \ microsoft \ windows \ microsoft \ micro$