Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3313, Task ID: 760

Task ID: 760 Risk Level: 10

Date Processed: 2016-05-18 10:34:55 (UTC)

Processing Time: 62.34 seconds IntelliVM Virtual Environment:

Execution Arguments: "c:\windows\temp\85d88c75b5c443841ecdd1c4079f040c.exe"

Sample ID: Type: basic admin Owner:

85d88c75b5c443841ecdd1c4079f040c Label:

2016-05-18 10:30:49 (UTC) Date Added: PE32:win32:gui File Type:

File Size: 94208 bytes

85d88c75b5c443841ecdd1c4079f040c MD5:

29c8729c05a22b46200c707b26c5704e746571bef6bc4af018bc09ca4887e67e SHA256:

Description: None

Pattern Matching Results

Modifies registry autorun entries

10 Creates malicious events: Vobfus [Worm]

5 PE: Contains compressed section

5 Adds autostart object

5 Creates process in suspicious location

Process/Thread Events

C:\WINDOWS\Temp\85d88c75b5c443841ecdd1c4079f040c.exe Creates process:

["c:\windows\temp\85d88c75b5c443841ecdd1c4079f040c.exe"]

C:\WINDOWS\Temp\85d88c75b5c443841ecdd1c4079f040c.exe [71] Creates process: Creates process: C:\Documents and Settings\Admin\peociak.exe ["C:\Documents and

Settings\Admin\peociak.exe"]

C:\Documents and Settings\Admin\peociak.exe [71] Creates process:

PID:260 C:\WINDOWS\Temp\85d88c75b5c443841ecdd1c4079f040c.exe Writes to process: PID:1860 C:\Documents and Settings\Admin\peociak.exe Writes to process: C:\WINDOWS\Temp\85d88c75b5c443841ecdd1c4079f040c.exe Terminates process:

Terminates process: C:\Documents and Settings\Admin\peociak.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

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

1957994488-1003

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

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

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

Creates mutex: \BaseNamedObjects\A

\BaseNamedObjects\ZonesCounterMutex Creates mutex:

Creates mutex: $\verb|\BaseNamedObjects\ZoneAttributeCacheCounterMutex| \\$ \BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex Creates event: \BaseNamedObjects\userenv: User Profile setup event

\BaseNamedObjects\C:?WINDOWS?TEMP?85D88C75B5C443841ECDD1C4079F040C.EXE Creates semaphore:

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} Creates semaphore: Creates semaphore: \BaseNamedObjects\C:?DOCUMENTS AND SETTINGS?ADMIN?PEOCIAK.EXE

File System Events

Creates: C:\Documents and Settings\Admin\peociak.exe Opens:

C:\WINDOWS\Prefetch\85D88C75B5C443841ECDD1C4079F0-283EB27F.pf

Opens: C:\Documents and Settings\Admin Opens: C:\WINDOWS\system32\msvbvm60.dll Opens: C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\system32\rpcss.dll Opens: C:\WINDOWS\svstem32\MSCTF.dll Opens: C:\WINDOWS\system32\sxs.dll C:\WINDOWS\system32\MSCTFIME.IME Opens:

C:\WINDOWS\Temp\85d88c75b5c443841ecdd1c4079f040c.exe Opens:

Opens: C:\WINDOWS\system32\apphelp.dll Opens: C:\WINDOWS\AppPatch\sysmain.sdb

```
C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C: \setminus
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\windows\temp\85d88c75b5c443841ecdd1c4079f040c.exe.Manifest
 Opens:
                         C:\WINDOWS\WINHELP.INI
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\shell32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\shell32.dll.124.Config
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\WindowsShell.Config
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\Documents and Settings\Admin\peociak.exe
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\Documents and Settings
 Opens:
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users
 Opens:
                         C:\Documents and Settings\All Users\Documents\desktop.ini
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
                         C:\WINDOWS\system32\urlmon.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\peociak.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\PEOCIAK.EXE-38B50E87.pf
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
```

Opens: C:\WINDOWS\Pretetcn\PEOCIAK.EXE-38BS
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\nnetcfg.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\system32\dnsapi.dll

Opens: Opens: C:\WINDOWS\system32\dnsapi.dll Opens: C:\WINDOWS\system32\iphlpapi.dll C:\WINDOWS\system32\winrnr.dll Opens: Opens: C:\WINDOWS\system32\drivers\etc\hosts Opens: C:\WINDOWS\system32\rsaenh.dll C:\WINDOWS\system32\crypt32.dll Opens: Opens: C:\WINDOWS\system32\rasadhlp.dll Opens: C:\WINDOWS\system32\MSIMTF.dll

Writes to: C:\Documents and Settings\Admin\peociak.exe

Reads from: C:\WINDOWS\Temp\85d88c75b5c443841ecdd1c4079f040c.exe
Reads from: C:\Documents and Settings\Admin\My Documents\desktop.ini
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\peociak.exe
Reads from: C:\WINDOWS\system32\drivers\etc\hosts

Reads from: C:\WINDOWS\system32\rsaenh.dll

Network Events

| DNS query: | ns1.boxonline1.com |
|---------------------|--------------------|
| DNS query: | ns1.boxonline1.net |
| DNS query: | ns1.boxonline1.org |
| DNS query: | ns1.boxonline2.com |
| DNS query: | ns1.boxonline2.net |
| DNS query: | ns1.boxonline2.org |
| DNS query: | ns1.boxonline3.com |
| DNS query: | ns1.boxonline3.net |
| DNS query: | ns1.boxonline3.org |
| 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: | <pre>HKCU\software\microsoft\windows\currentversion\explorer\shell folders</pre> |
| Creates key: | |
| HKCU\software\micro | osoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7- |
| 806d6172696f}\ | |
| Creates key: | <pre>HKLM\software\microsoft\windows\currentversion\explorer\user shell</pre> |
| folders | |
| Creates key: | <pre>HKLM\software\microsoft\windows\currentversion\explorer\shell folders</pre> |
| Creates key: | <pre>HKCU\software\microsoft\windows\currentversion\run\</pre> |
| Creates key: | <pre>HKCU\software\microsoft\windows\currentversion\explorer\advanced\</pre> |
| Creates key: | <pre>HKLM\software\policies\microsoft\windows\windowsupdate\au</pre> |
| Creates key: | HKLM\software |

Creates key: HKLM\software\policies

HKLM\software\policies\microsoft Creates kev:

HKLM\software\policies\microsoft\windows Creates kev:

HKLM\software\policies\microsoft\windows\windowsupdate Creates key: Creates kev: HKLM\system\currentcontrolset\services\tcpip\parameters

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

options\85d88c75b5c443841ecdd1c4079f040c.exe

Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key: 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\software\microsoft\windows nt\currentversion\image file execution

options\gdi32.dll

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

options\user32.dll

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

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

options\imm32.dll

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 kev: 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: options\advapi32.dll

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

Opens kev:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll

Opens key:

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

options\ole32.dll

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

options\oleaut32.dll

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

options\msvbvm60.dll

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

Opens key: $\label{lem:hklm} \mbox{HKLM} \mbox{$\tt MKLM} \mbox$ Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon

HKI M\ Opens key:

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

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046}

HKLM\software\microsoft\oleaut Opens kev:

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

Opens key: HKCU\

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

HKCU\control panel\desktop Opens key:

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\85d88c75b5c443841ecdd1c4079f040c.exe

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

HKCU\keyboard layout\toggle Opens key: Opens key: HKLM\software\microsoft\ctf\

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

options\sxs.dll

Opens key: HKLM\system\setup

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

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

options\version.dll

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ Opens key:

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

Opens key: HKLM\system\currentcontrolset\control\nls\codepage

Opens key: HKLM\software\microsoft\vba\monitors

Opens key: Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\apphelp.dll

Opens key: HKLM\system\wpa\tabletpc HKLM\system\wpa\mediacenter Opens key:

 ${\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus app compatflags \setminus layers}$ Opens key:

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\85d88c75b5c443841ecdd1c4079f040c.exe

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

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths 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-9b89edd5fbde1328} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91} 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\{94e3e076-8f53-42a5-8411-085bcc18a68d3 Opens key: b91490411bfc} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 131072 \ paths$ Opens kev: 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 kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths$ Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones Opens kev: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus paths$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens key:

 $\label{lem:hkcu} HKCU \software \policies \microsoft \windows \safer \code identifiers \code \normalfong \normal$

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

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

 $\label{lem:hkcu} HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones \\ Opens\ key:$

 $\label{lem:hkcu} HKCU\software\policies\microsoft\windows\safer\codeidentifiers\codeidentifi$

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

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

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

Opens key: HKLM\software\microsoft\windows

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

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

options\shlwapi.dll

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

options\shell32.dll

Opens key:

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: HKLM\software\microsoft\windows nt\currentversion\languagepack

Opens key: HKLM\software\microsoft\windows nt\currentversion\impac file opension

HKLM\software\microsoft\windows nt\currentversion\impac file opension

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

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

options\userenv.dll

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 key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003

Opens key: HKLM\system\currentcontrolset\services\disk\enum

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ 85d88c75b5c443841ecdd1c4079f040c. exemple \ description \ applications \ a$

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

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

options\netapi32.dll

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

Opens key: HKLM\software\microsoft\rpc

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

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key:

a2d8-08002b30309d}

Opens key: HKCU\software\classes\

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

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

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

Opens key: HKCU\software\classes\exefile\curver

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

Opens key: HKCU\software\classes\exefile\shellex\iconhandler

Opens key: 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

Opens key: HKCR\exefile\clsid
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 kev:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

Opens key:

11e3-9fc7-806d6172696f}\

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver

Opens key: HKCR\directory\curver

Opens key: HKCR\directorv\

HKCU\software\classes\directory\shellex\iconhandler Opens kev:

HKCR\directory\shellex\iconhandler Opens key: Opens key: HKCU\software\classes\directory\clsid

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

HKCR\folder Opens key:

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

HKCR\folder\clsid Opens key:

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus shell execute hooks$ Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-

00c04fd91972}\inprocserver32

Opens key: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32 Opens key: HKLM\software\microsoft\windows\currentversion\policies\associations HKCU\software\microsoft\windows\currentversion\policies\associations Opens kev:

Opens key: HKCU\software\classes\.ade

Opens key: HKCR\.ade

HKCU\software\classes\.adp Opens key:

Opens key: HKCR\.adp

Opens key: HKCU\software\classes\.app

Opens kev: HKCR\.app

Opens key: HKCU\software\classes\.asp

Opens key: HKCR\.asp

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

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

HKCU\software\classes\.cpl Opens key:

Opens key: HKCR\.cpl

Opens key: HKCU\software\classes\.crt

Opens key: HKCR\.crt

HKCU\software\classes\.csh Opens key:

Opens kev: HKCR\.csh

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

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

options\clbcatq.dll

HKLM\software\microsoft\com3\debug Opens kev:

HKLM\software\classes Opens key:

Opens key: HKU\

HKCR\clsid Opens key:

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\treatas

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key:

00c04fb6bfc4}\inprocserver32

Opens key: $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32$

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserverx86

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86 Opens key:

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens kev:

00c04fb6bfc4}\localserver32

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4\inprochandler32

Opens key: $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid$

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens kev:

00c04fb6bfc4}\inprochandlerx86

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86 Opens kev:

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key:

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: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

```
settings
```

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings Opens kev: HKLM\software\policies\microsoft\windows\currentversion\internet

settings

Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown HKLM\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_protocol_lockdown

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

settings\

Opens kev: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: $\label{lem:hkcu} \verb+KKCU\software\policies\microsoft\internet\ explorer\main\feature control$

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol HKCU\software\microsoft\internet explorer\main\featurecontrol Opens kev: 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\

 $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$ Opens key:

settings\zonemap\domains\

HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev:

settings\zonemap\ranges\

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

settings\zonemap\ranges\

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_unc_savedfilecheck

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap\

Opens key: HKCU\software\microsoft\internet

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 HKCU\software\policies Opens key: Opens key: HKCU\software Opens key: HKLM\software

HKCU\software\microsoft\windows\currentversion\internet Opens key:

settings\zonemap\ranges\

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap\protocoldefaults\

HKCU\software\microsoft\windows\currentversion\internet Opens key:

settings\zonemap\domains\

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

settings\zonemap\domains\

HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\domains\msn.com

Opens kev:

HKLM\software\microsoft\windows\currentversion\internet settings\zonemap\domains\msn.com\related

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination Opens kev: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination HKCU\software\microsoft\internet explorer\ietld Opens kev:

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 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

HKLM\software\microsoft\internet Opens key:

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

HKLM\software\policies\microsoft\internet explorer\security Opens key:

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 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\software\policies\microsoft\windows\currentversion\internet

settings\zones\

Opens key: $\label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\currenters$

settings\zones\

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

```
settings\zones\0
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\0
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens key:
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\zones\1
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\3
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 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
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
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
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
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
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
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 key:
settings\lockdown_zones\4
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
                          HKCU\software\classes\exefile\shell
 Opens kev:
                          HKCR\exefile\shell
 Opens key:
 Opens key:
                          HKCU\software\classes\exefile\shell\open
 Opens key:
                          HKCR\exefile\shell\open
                          HKCU\software\classes\exefile\shell\open\command
 Opens key:
 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\peociak.exe
 Opens key:
                          HKCU\software\classes\exefile\shell\open\ddeexec
 Opens key:
                          HKCR\exefile\shell\open\ddeexec
 Opens key:
                          HKCU\software\classes\applications\peociak.exe
 Opens kev:
                          HKCR\applications\peociak.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 key:
                          HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\peociak.exe
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
```

options\peociak.exe

HKLM\software\microsoft\ctf\compatibility\peociak.exe Opens kev:

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

options\ws2help.dll

Opens kev:

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

options\ws2_32.dll

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens key:

Opens key:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 000000000010$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key:

Opens key:

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

options\mswsock.dll

Opens key:

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

HKLM\software\microsoft\rpc\securityservice

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

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

options\dnsapi.dll

 $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ dns \+ cache \+ parameters$ Opens key: Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

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

options\iphlpapi.dll

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:

c7d49d7cecdc}

Opens kev: options\wldap32.dll

Opens key: HKLM\svstem\currentcontrolset\services\ldap

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

Opens key:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wicrosoft \label{lem:hklm} software \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} wicrosoft \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} \label{lkm} \label{lkm}$

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

cryptographic provider

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll

Opens key:

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

Opens key: HKLM\software\microsoft\cryptography\offload Opens key: HKLM\system\currentcontrolset\control\wmi\security

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

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

Oueries value:

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

Queries value: HKLM\system\currentcontrol\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Oueries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[85d88c75b5c443841ecdd1c4079f040c]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ime

compatibility[85d88c75b5c443841ecdd1c4079f040c]

Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]

Queries value: HKLM\system\currentcontrolset\control\session

manager[criticalsectiontimeout]

Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]

Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]

Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableall]

Queries value: HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableallforole32]

Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKLM\system\currentcontrol\set\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]

Queries value: HKLM\system\currentcontrolset\control\session

manager\appcompatibility[disableappcompat]

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

Queries value:

 $HKLM \verb| software \verb| policies \verb| microsoft \verb| windows \verb| safer \verb| code identifiers [authenticode enabled] |$

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

Queries value:

 $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33\}[itemdata]$

Queries value:

Queries value:

Queries value:

Queries value:

Queries value:

 $HKLM \ software \ `microsoft \ `safer \ ode identifiers \ `0 \ hashes \ \{349d35ab-37b5-462f-9b89-edd5fbde 1328\} \ [saferflags]$

Queries value:

Queries value:

 $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}\[hashalg]$

Queries value:

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

Queries value:

 $\label{thm:local-beta-def} $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\}[saferflags]}$

Queries value:

 $\label{thm:local-bound} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}\[itemdata]\]$

Queries value:

 $\label{thm:local-bound} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}\[hashalg]$

Queries value:

Oueries value:

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

Queries value:

085bcc18a68d}[itemdata]

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[cache] Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [log filename]$

HKLM\system\setup[systemsetupinprogress] Queries value: HKCU\control panel\desktop[smoothscroll] Oueries value:

Oueries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [enable balloon tips]$

HKLM\software\microsoft\windows Queries value:

nt\currentversion\winlogon[userenvdebuglevel]

HKLM\software\microsoft\windows Queries value:

nt\currentversion\winlogon[chkaccdebuglevel]

Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value:

folders[personal]

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

folders[local settings]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\winlogon[rsopdebuglevel]

HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003[profileimagepath]

Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]

HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]

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

Oueries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

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

Oueries value:

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

Oueries value:

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

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

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Oueries value:

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

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] Oueries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Oueries value:

409d6c4515e9}[drivemask]

Queries value:

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

Queries value: HKCR\.exe[]

Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[forceactive desktop on]]$

Queries value:

```
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                                                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidden \cite{tabular} \end{tabular}
   Queries value:
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [filter]
   Queries value:
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Queries value:
Queries value:
                                                   HKCR\exefile[docobject]
   Oueries value:
                                                   HKCR\exefile[browseinplace]
                                                    HKCR\exefile[isshortcut]
   Queries value:
                                                   HKCR\exefile[alwaysshowext]
   Oueries value:
   Oueries value:
                                                   HKCR\exefile[nevershowext]
                                                    HKLM\system\wpa\pnp[seed]
   Queries value:
   Queries value:
                                                    HKLM\system\setup[osloaderpath]
   Oueries value:
                                                   HKLM\system\setup[systempartition]
                                                    HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:
   Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
   Oueries value:
                                                   HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
   Queries value:
                                                    HKLM\software\microsoft\windows\currentversion[devicepath]
   Oueries value:
                                                   HKLM\software\microsoft\windows\currentversion\setup[loglevel]
   Queries value:
                                                   HKLM\software\microsoft\windows\currentversion\setup[logpath]
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Oueries value:
                                                   HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Queries value:
HKCU \ software \ icrosoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-five \ for \ f
11e3-9fc7-806d6172696f}[data]
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ mountpoints 2 \ cpc \ \ \ \{f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c2-6bc4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9026c4-f9006c4-f906c4-f906c4-f906c4-f906c4-f906c4-f906c4-f906c4-f906c4-f906c4-f906c4-f906c4-f906c4-f90
11e3-9fc7-806d6172696f}[generation]
                                                    HKCR\directory[docobject]
   Oueries value:
                                                    HKCR\directory[browseinplace]
   Queries value:
   Queries value:
                                                    HKCR\directory[isshortcut]
   Oueries value:
                                                   HKCR\directory[alwaysshowext]
                                                    HKCR\directory[nevershowext]
   Queries value:
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
   Queries value:
                                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell
folders[common documents]
                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[desktop]
                                                    HKLM\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[common desktop]
                                                   HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\\\\inprocserver32[]
   Queries value:
   Queries value:
                                                   HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
   Queries value:
                                                   HKCR\.asp[]
                                                    HKCR\.bat[]
   Queries value:
   Oueries value:
                                                    HKCR\.cer[]
   Oueries value:
                                                   HKCR\.chm[]
   Queries value:
                                                    HKCR\.cmd[]
   Oueries value:
                                                    HKCR\.com[]
```

Queries value:

HKCR\.cpl[]

Oueries value: HKCR\.crt[] HKLM\software\microsoft\com3[com+enabled] Oueries value: Oueries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess] Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject] Oueries value: HKLM\software\microsoft\com3[regdbyersion] Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[inprocserver32] HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[] Oueries value: Oueries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid] Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel] Queries value: $\label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet$ settings[disableimprovedzonecheck] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[85d88c75b5c443841ecdd1c4079f040c.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow] HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh] Queries value: Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[enablepunycode] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[enablepunycode] Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\0[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\1[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\4[flags] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[85d88c75b5c443841ecdd1c4079f040c.exe] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature localmachine lockdown[*1 Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[85d88c75b5c443841ecdd1c4079f040c.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[cache] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cookies] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1806] HKCR\exefile\shell[1 Oueries value: HKCR\exefile\shell\open\command[] Queries value: HKCR\exefile\shell\open\command[command] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[flags] $\label{lem:hklm} \mbox{ HKLM} \mbox{ hicrosoft} \mbox{ windows nt} \mbox{ currentversion} \mbox{ profilelist} \mbox{ s-1-5-21-1} \mbox{ of tware} \mbox{ windows nt} \mbox{ of tware} \mbox{ of$ Queries value: 1757981266-507921405-1957994488-1003[state] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[userpreference] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Queries value: 1757981266-507921405-1957994488-1003[centralprofile] Queries value: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \$ 1757981266-507921405-1957994488-1003[profileloadtimelow] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileloadtimehigh] HKCU\software\microsoft\windows\shellnoroam\muicache[langid] Oueries value: Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and settings\admin\peociak.exe] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist] Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]

Oueries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[disallow run]$

Oueries value:

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

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[peociak]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ime

compatibility[peociak]

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:

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

```
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 00000000000003 [version]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog\_entries \ (00000000003[storesserviceclass info]) \ (catalog\_entries) \ 
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:
                                    HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                                    HKLM\svstem\currentcontrolset\services\winsock\parameters[transports]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
HKLM \verb| system| current control set \verb| services| tcpip| parameters [usedomain named evolution]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[guervipmatching]
  Queries value:
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]
   Queries value:
                                            HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Oueries value:
                                             HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
                                            {\tt HKLM \ } system \ \verb| current control set \ \verb| services \ \verb| dns cache \ \verb| parameters [max cachettl]|
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
   Queries 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\linkage[bind]
   Queries value:
   Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[enabledhcp]
   Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[leaseobtainedtime]
   Queries value:
c7d49d7cecdc}[leaseterminatestime]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
   Queries value:
c7d49d7cecdc}[queryadaptername]
  Oueries value:
c7d49d7cecdc}[disableadapterdomainname]
   Queries value:
c7d49d7cecdc}[registrationenabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
   Oueries value:
c7d49d7cecdc}[registrationmaxaddresscount]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
   Oueries value:
c7d49d7cecdc}[domain]
   Queries value:
c7d49d7cecdc}[dhcpdomain]
   Oueries value:
c7d49d7cecdc}[ipautoconfigurationenabled]
   Queries value:
c7d49d7cecdc}[addresstype]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
   Oueries value:
                                            HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                                            HKLM\system\currentcontrolset\services\ldap[ldapclientintegritv]
   Oueries value:
   Oueries value:
                                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                                            HKLM \ software \ \verb|microsoft| cryptography \ defaults \ \verb|provider| microsoft| strong|
   Oueries value:
cryptographic provider[image path]
```

HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value:

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

Oueries value:

ab78-1084642581fb]

Oueries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-

0000-0000000000001 Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and

settings\admin\peociak.exe]

HKCU\software\microsoft\windows\currentversion\run[peociak] Sets/Creates value:

Sets/Creates value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]$

Sets/Creates value: HKLM\software\policies\microsoft\windows\windowsupdate\au[noautoupdate]

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

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

folders[personal] Value changes:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus \{f90255c2-6bc4-11e3-9fc7-bc$

806d6172696f}[baseclass]

 $\label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell$ Value changes:

folders[common documents]

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

folders[desktop]

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

folders[common desktop]

 $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$ Value changes:

settings\zonemap[proxybypass]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[uncasintranet]

HKCU\software\microsoft\windows\currentversion\internet Value changes:

settings\zonemap[autodetect]

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

folders[cache]

HKCU\software\microsoft\windows\currentversion\explorer\shell

Value changes: folders[cookies]

HKCU\software\microsoft\windows\currentversion\run[peociak] Value changes:

Value changes:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]

Value changes: HKLM\software\policies\microsoft\windows\windowsupdate\au[noautoupdate]