# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 114, Task ID: 455

Task ID: 455 Risk Level: 7

Date Processed: 2016-04-28 12:59:27 (UTC)

Processing Time: 61.08 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\71985e8a4de40ddc1151fafb929b5614.exe"

Sample ID: 114
Type: basic
Owner: admin

Label: 71985e8a4de40ddc1151fafb929b5614

Date Added: 2016-04-28 12:45:01 (UTC)

File Type: PE32:win32:gui File Size: 994608 bytes

MD5: 71985e8a4de40ddc1151fafb929b5614

SHA256: ad48111f30408fba6fe47b84d149e73078a391b9be4c27b334212071dcb6c88b

Description: None

## Pattern Matching Results

3 Long sleep detected

- 6 Renames file on boot
- 5 Creates process in suspicious location
- PE: Nonstandard section
- 3 HTTP connection response code 200 (success) [HTTP, POST, GET, web, network, response code]
- 1 YARA score 1
- Signed by adware producer [Adware, PUA]
- 3 Connects to local host
- 4 Packer: NSIS [Nullsoft Scriptable Install System]

#### Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable
Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

#### Process/Thread Events

```
C:\WINDOWS\Temp\71985e8a4de40ddc1151fafb929b5614.exe
["c:\windows\temp\71985e8a4de40ddc1151fafb929b5614.exe"]
                                        C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\BI.exe { "json_send_time" : "28/4/2016 14:59:51:357" , "product_id_version" : "" , "product_type" : "" , "product_id" : "" , "offer_id" : "85063" , "user_type" : "NULL" , "result" : "Success" , "user_operating_system_bits" : "" , "current_default_search" : "" , "current_homepage" : "" , "current_toolbars" : "" ,
"attempt_number": "1", "is_silent": "", "user_ms_dotnet_framework_ver": "",
"user_acount_type": "", "user_ie_version": "", "user_default_browser_version": "",
"user_default_browser": "", "user_service_pack": "", "user_operating_system": "",
"revision_number": "0", "build_id": "00000000", "dm_version": "1.3.7.9_NoStatic.130521.01",
"bundle_id": "8dea43ae-643c-435c-8c80-371666b121ed", "machine_user_id": "{4D594B68-7E93-4DA2-
B705-E56910C4AE2A}" , "send_attempt" : "0" , "channel_id" : "" , "installation_session_id" :
"464BECC8-64BE-44B8-9BF5-0BEABBE79862" , "publisher_internal_id" : "1" , "publisher_id" : "Brothersoft" , "publisher_account_id" : "Brothersoft" , "order" : "1.0" , "phase" : "Init" , "Is_Test" : "0" }]
  Creates process:
                                         C: \DOCUME \sim 1 \land Admin \land LOCALS \sim 1 \land Temp \land sh3.tmp \land BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\BI.exe { "user_ie_security_level" : "Unknown-0"
"json_send_time" : "28/4/2016 15:0:59:98" , "internal_error_description" : "HttpPost to CMS
result- try3: Error navigating ( in GetNavigateError error code is -2146697211) to url:
http://cms.distributionengine.conduit-services.com//MainOffer/85004/?CurrentStep=1"
"internal_error_number": "3", "is_parallel": "0", "mrs_id": "-1", "vector_id": "581222", "rule_id": "580630", "product_id_version": "", "product_type": "", "product_id": "", "offer_id": "85063", "general_status_code": "6", "duration_details": "InitPluginsDir:0
initializeParams:331 load_BITool:180 send_BI_Init:140 load_DownloadACC:60 retrieveUISource:10
unpack_webappfolder:0 unpack_icon:0 RetrieveMainOfferKey:0 unpack_OpenCandyDll:271
load_webapphost:0 unpack_ProxyInstaller:20 navigate_loadingUI:1111 navigateAsync_constMainOffer:0
BuildUserProfile:20 retrieve cid:0 callService1:62594 parse_ResponseXml:2954
init_external_offer:0 DiscoverUserAgent:181 " , "phase_duration" : "" , "error_details" : "55
Failed to communicate with CMS for main offer" , "result" : "Error" ,
"user_operating_system_bits" : "32" , "current_default_search" :
"http://search.live.com/results.aspx?q={searchTerms}&src=IE-SearchBox&Form=IE8SRC"
"current_homepage": "about:blank", "current_toolbars": "", "attempt_number": "1",

"is_silent": "0", "user_ms_dotnet_framework_ver": "3.5", "user_acount_type": "",

"user_ie_version": "8.0.6001.18702", "user_default_browser_version": "8.0.6001.18702",

"user_default_browser": "IEXPLORE.EXE", "user_service_pack": "3.0", "user_operating_system":

"Microsoft Windows XP", "revision_number": "0", "build_id": "000000000", "dm_version":
"1.3.7.9_NoStatic.130521.01" , "bundle_id" : "8dea43ae-643c-435c-8c80-371666b121ed"
"machine_user_id" : "{4D594B68-7E93-4DA2-B705-E56910C4AE2A}" , "send_attempt" : "0"
"channel_id" : "" , "installation_session_id" : "464BECC8-64BE-44B8-9BF5-0BEABBE79862"
```

```
"publisher_internal_id" : "1" , "publisher_id" : "Brothersoft" , "publisher_account_id" : "Brothersoft" , "order" : "2.0" , "phase" : "InitComplete" , "Is_Test" : "0" }]
```

RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service: Terminates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\BI.exe

### Named Object Events

```
Creates mutex:
                                                    \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003
                                                   \verb|\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1808| in the compart of the compart
   Creates mutex:
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
                                                   \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-
   Creates mutex:
507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
                                                   \BaseNamedObjects\oleacc-msaa-loaded
   Creates mutex:
   Creates mutex:
                                                   \BaseNamedObjects\ActiveSetupMutexId
   Creates mutex:
                                                   \BaseNamedObjects\c:!documents and settings!admin!local
settings!temporary internet files!content.ie5!
                                                   \BaseNamedObjects\c:!documents and settings!admin!cookies!
   Creates mutex:
   Creates mutex:
                                                   \BaseNamedObjects\c:!documents and settings!admin!local
settings!history!history.ie5!
                                                   \verb|\BaseNamedObjects\WininetConnectionMutex| \\
   Creates mutex:
   Creates mutex:
                                                   \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex
   Creates mutex:
                                                   \BaseNamedObjects\ZonesCounterMutex
                                                   \BaseNamedObjects\ZoneAttributeCacheCounterMutex
   Creates mutex:
   Creates mutex:
                                                   \BaseNamedObjects\ZonesCacheCounterMutex
   Creates mutex:
                                                   \BaseNamedObjects\ZonesLockedCacheCounterMutex
                                                   \BaseNamedObjects\MSIMGSIZECacheMutex
   Creates mutex:
   Creates mutex:
                                                   \BaseNamedObjects\_!SHMSFTHISTORY!_
   Creates mutex:
                                                   \BaseNamedObjects\c:!documents and settings!admin!local
settings!history!history.ie5!mshist012016042820160429!
   Creates mutex:
                                                   \BaseNamedObjects\MSCTF.Shared.MUTEX.AHH
   Creates event:
                                                   \BaseNamedObjects\userenv: User Profile setup event
   Creates semaphore:
                                                   \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
   Creates semaphore:
                                                   \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
                                                    \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
   Creates semaphore:
```

\BaseNamedObjects\OleDfRoot000025BB5

## File System Events

Creates semaphore:

File System Events		
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsj1.tmp	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsn2.tmp	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp	
Creates:	C:\DOCUME~1	
Creates:	C:\DOCUME~1\Admin	
Creates:	C:\DOCUME~1\Admin\LOCALS~1	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\System.dll</pre>	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\System.dll	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsh3.tmp\webapphost.dll		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\BI.exe</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsh3.tmp\DM_loader.gif		
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsh3.tmp\DownloadACC.exe		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\Failed.htm</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\icon.png</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsh3.tmp\OCSetupHlp.dll		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsu4.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nss5.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp</pre>	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm6.tmp	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp\inetc.dll</pre>	
Creates:	<pre>C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\webapphost.dll</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsh3.tmp\ProxyInstaller.exe		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp\a.txt</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\~DF5BB8.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\inetc.dll</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\offer.xml</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temporary Internet</pre>	
Files\Content.IE5\QXMNQBKF\navcancl[1]		
Creates:	<pre>C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm6.tmp\inetc.dll</pre>	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temporary Internet	
Files\Content.IE5\UH4D6D6X\navcancl[1]		

```
Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\background_gradient[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\UH4D6D6X\bullet[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\UH4D6D6X\background_gradient[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\info_48[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\background_gradient[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\UH4D6D6X\down[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[2]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\OXMNOBKF\down[1]
 Creates
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_webOC[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\CXCXW1MR\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\OXMNOBKF\down[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\CXCXW1MR\background_gradient[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\xml.dll
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\xml.dll
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\nsArray.dll
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\nsArray.dll
 Creates:
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\info_48[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\CXCXW1MR\bullet[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsp7.tmp
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsx8.tmp
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp
                         C: \DOCUME \sim 1 \land Admin \land LOCALS \sim 1 \land Temp \land nsz9.tmp
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp\inetc.dll
 Creates:
 Creates:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\History\History.IE5\MSHist012016042820160429\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp\a.txt
 Creates:
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsz9.tmp\inetc.dll
                         \verb|C:\WINDOWS\Prefetch\71985E8A4DE40DDC1151FAFB929B5-0531102D.pf| \\
 Opens:
 Opens:
                         C:\Documents and Settings\Admin
                         C:\WINDOWS\svstem32\imm32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shell32.dll
```

```
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:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\Temp\71985e8a4de40ddc1151fafb929b5614.exe
 Opens:
 Opens:
                         C:\windows\temp\71985e8a4de40ddc1151fafb929b5614.exe.124.Manifest
 Opens:
                         C:\WINDOWS\svstem32\comctl32.dll
                         C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\COMCTL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
                         C:\WINDOWS\system32\shfolder.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\
 Opens:
                         C:\Documents and Settings
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsj1.tmp
 Opens:
 Opens:
                         C:\WINDOWS\Temp\b17ee106-6102-417c-b654-69db9480d5a8
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\System.dll
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nsh3.tmp\webapphost.dll
 Opens:
                         \label{locals-locals-locals-locals-locals} C: \verb|\DOCUME-1| Admin\\ LOCALS-1\\ Temp\\ nsh3.tmp\\ we bapphost.dll.2.Manifest
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\webapphost.dll.2.Config
 Opens:
                         C:\WINDOWS\system32\winspool.drv
 Opens:
 Opens:
                         C:\WINDOWS\system32\oledlg.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
                         C:\WINDOWS\system32\msasn1.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\oleacc.dll
 Opens:
                         C:\WINDOWS\system32\msvcp60.dll
 Opens:
                         C:\WINDOWS\system32\oleaccrc.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\webapphost.dll.1000.Manifest
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsh3.tmp\BI.exe}
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsh3.tmp\BI.exe.Manifest
                         C:\WINDOWS\Prefetch\BI.EXE-127C2367.pf
 Opens:
 Opens:
                         \label{locals-1} C: \DOCUME $$^1\Lambda = 1.4. Manifest $$
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsu4.tmp
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp\inetc.dll
 Opens:
                         C:\WINDOWS\Fonts\sserife.fon
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
                         C:\AUTOEXEC.BAT
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
```

```
Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\asycfilt.dll
 Opens:
                         C:\WINDOWS\system32\clbcatg.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\icon.png
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsh3.tmp\inetc.dll}
 Opens:
                         C:\WINDOWS\system32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
                         C:\WINDOWS
 Opens:
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
                         C:\WINDOWS\svstem32\wshtcpip.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\navcanc1[2]
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp\a.txt
 Opens:
 Opens:
                         C:\WINDOWS\system32\psapi.dll
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm6.tmp\
 Opens:
                         C:\WINDOWS\system32\mlang.dll
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\navcancl[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\navcancl[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         C:\WINDOWS\system32\iepeers.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Config
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
 Opens:
                         C:\WINDOWS\system32\jscript.dll
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\info 48[1]
                         C:\WINDOWS\system32\imgutil.dll
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\QXMNQBKF\bullet[1]
                         {\tt C:\WINDOWS\system32\pngfilt.dll}
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\background_gradient[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info 48[2]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\info_48[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[2]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
                         C:\WINDOWS\Fonts\SEGOEUI.TTF
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\CXCXW1MR
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\background_gradient[2]
                         C:\WINDOWS\Fonts\wingding.ttf
 Opens:
 Opens:
                         C:\WINDOWS\system32\en-US\mshtml.dll.mui
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\info_48[2]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\down[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\down[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_web0C[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\down[2]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\xml.dll
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\offer.xml
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\nsArray.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\background_gradient[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\info_48[1]
 Opens:
                         C:
 Opens:
                         C:\WINDOWS\system32\config
 Opens:
                         C:\WINDOWS\system32\drivers
 Opens:
                         C:\WINDOWS\system32\drivers\etc
                         C:\WINDOWS\Temp
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
 Opens:
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
                         C:\WINDOWS\system32\user32.dll
                         C:\WINDOWS\system32\gdi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\advapi32.dll
 Opens:
                         C:\WINDOWS\system32\rpcrt4.dll
 Opens:
                         C:\WINDOWS\system32\secur32.dll
 Opens:
                         C:\WINDOWS\system32\msvcrt.dll
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
 Opens:
                         C:\WINDOWS\system32\ctype.nls
 Opens:
                         C:\WINDOWS\system32\sortkey.nls
                         C:\WINDOWS\system32\wininet.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\normaliz.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\iertutil.dll
 Opens:
                         C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM
 Opens:
                         C:\WINDOWS\system32\userenv.dll
 Opens:
                         C:\WINDOWS\Temp\b17ee106-6102-417c-b654-69db9480d5a8\96d_inetc.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\Failed.htm
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
                         C:\WINDOWS\Fonts\arialbd.ttf
 Opens:
                         C:\WINDOWS\Fonts\verdana.ttf
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsp7.tmp
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp\inetc.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
```

```
Settings\History\History.IE5\MSHist012016042820160429
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012016042820160429\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp\a.txt
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsz9.tmp\
 Opens:
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn2.tmp
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\System.dll
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\nsh3.tmp\webapphost.dll
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\BI.exe
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\nsh3.tmp\DM_loader.gif
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nsh3.tmp\DownloadACC.exe
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\Failed.htm
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\icon.png
                         C:\Documents and Settings\Admin\Local Settings\Temp\nss5.tmp
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp\inetc.dll
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nsh3.tmp\OCSetupHlp.dll
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\nsh3.tmp\ProxyInstaller.exe
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\inetc.dll
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\navcancl[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Writes to:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\info 48[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\down[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_webOC[2]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\bullet[2]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_web0C[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Writes to:
Files\Content.IE5\CXCXW1MR\httpErrorPagesScripts[1]
```

```
C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Writes to:
Files\Content.IE5\QXMNQBKF\down[2]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Writes to:
Files\Content.IE5\CXCXW1MR\background_gradient[1]
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\offer.xml
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\xml.dll
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\nsArray.dll
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Writes to:
Files\Content.IE5\CXCXW1MR\info_48[1]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\bullet[1]
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsx8.tmp
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp\inetc.dll
                                   C:\Documents and Settings\Admin\Local
  Writes to:
Settings \verb|\History\E5| MSH is to 12016042820160429 \verb|\index.dat| at the setting and the set
                                   C:\WINDOWS\Temp\71985e8a4de40ddc1151fafb929b5614.exe
  Reads from:
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsn2.tmp
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\BI.exe
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nss5.tmp
  Reads from:
                                   C:\AUTOEXEC.BAT
  Reads from:
                                   C:\WINDOWS\system32\drivers\etc\hosts
  Reads from:
                                   C:\WINDOWS\system32\rsaenh.dll
                                   C:\WINDOWS\Registration\R00000000007.clb
  Reads from:
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\offer.xml
  Reads from:
                                   C:\WINDOWS\Prefetch\BI.EXE-127C2367.pf
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp\Failed.htm
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsx8.tmp
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsj1.tmp
  Deletes:
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsh3.tmp
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsu4.tmp
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\UH4D6D6X\navcanc1[2]
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp\a.txt
  Deletes:
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\nsm6.tmp\inetc.dll
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\navcancl[1]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[1]
                                   {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
  Deletes:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\UH4D6D6X\background gradient[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[1]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\QXMNQBKF\bullet[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\QXMNQBKF\background_gradient[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[2]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[2]
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Deletes:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[2]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[1]
                                   {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
  Deletes:
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[2]
  Deletes:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\UH4D6D6X\down[1]
```

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\QXMNQBKF\dnserrordiagoff\_web0C[2]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\CXCXW1MR\errorPageStrings[1]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\QXMNQBKF\bullet[2]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\QXMNQBKF\down[1]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\UH4D6D6X\dnserrordiagoff\_webOC[1]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\CXCXW1MR\httpErrorPagesScripts[1]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\QXMNQBKF\down[2]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\CXCXW1MR\background\_gradient[1]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\CXCXW1MR\info\_48[1]

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsp7.tmp

Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014033120140407\index.dat Deletes: C:\Documents and Settings\Admin\Local

Settings\History\History.IE5\MSHist012014033120140407

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp

Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014041220140413\index.dat Deletes: C:\Documents and Settings\Admin\Local

 $Settings \verb|\History\History\IE5\MSHist012014041220140413|$ 

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp\a.txt
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsz9.tmp\netc.dll

#### **Network Events**

DNS query: ude.conduit-data.com

DNS query: offering.service.distributionengine.conduit-services.com

DNS query: cms.distributionengine.conduit-services.com

DNS response: offering.service.distributionengine.ams.conduit-services.com ⇒

195.78.120.173

Connects to: 195.78.120.173:80
Connects to: 127.0.0.1:1054
Sends data to: 8.8.8.8:53

Sends data to: offering.service.distributionengine.ams.conduit-services.com:80

(195.78.120.173)

Receives data from: 0.0.0.0:0

Receives data from: offering.service.distributionengine.ams.conduit-services.com:80

(195.78.120.173)

## Windows Registry Events

Creates key:

 $\label{two-continuous} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \f 90255c2-6bc4-11e3-9fc7-806d6172696f \end{center} \\$ 

Creates key: HKCU\software\appdatalow\software\smartbar

Creates key: HKCU\software

Creates key: HKCU\software\appdatalow

Creates key: HKCU\software\appdatalow\software

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

folders

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

Creates key: HKLM\software\microsoft\tracing

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

folders

Creates key: HKCU\software\microsoft\windows nt\currentversion\winlogon

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

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

settings\connections

Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location

awareness

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached

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

Creates key: HKCU\software\conduit\distributionengine\1\offerhistory\755131

Creates key: HKCU\software\conduit

Creates key: HKCU\software\conduit\distributionengine
Creates key: HKCU\software\conduit\distributionengine\1

Creates key: HKCU\software\conduit\distributionengine\1\offerhistory Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042820160429

Creates key: HKCU\software\microsoft\internet explorer\main\windowssearch

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\71985e8a4de40ddc1151fafb929b5614.exe

Opens key: HKLM\system\currentcontrolset\control\terminal server

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

options\gdi32.dll

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

options\user32.dll

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

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens kev:

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

options\imm32.dll

 $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hicrosoft}\windows nt\currentversion} \mbox{$\mbox{image file execution}$} \\$ Opens key:

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\secur32.dll

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

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\image file execution

options\msvcrt.dll

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

options\shlwapi.dll

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

options\shell32.dll

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

options\comctl32.dll

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

options\ole32.dll

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

options\version.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ HKLM\system\currentcontrolset\control\error message instrument Opens kev:  $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} in the constant of the const$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility  $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows}} \ \ \mbox{nt\current\version\windows}$ Opens key:

Opens key:  $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + winlog on + current + version + version$ HKLM\ Opens kev:

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

Opens key: HKLM\svstem\setup

Opens key: HKCU\

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

Opens kev: HKCU\control panel\desktop

Opens key:

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

HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ language pack$ Opens key:

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\71985e8a4de40ddc1151fafb929b5614.exe

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

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

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

options\shfolder.dll

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

 $HKLM \label{loss} HKLM \label{loss} HKLM \label{loss} HKLM \label{loss} Software \label{loss} Windows \label{loss} Label{loss} HKLM \label{loss} HKLM \label{loss} Label{loss} HKLM \label{loss} Label{loss} Label{loss} HKLM \label{loss} Label{loss} Label{los$ 

a2d8-08002b30309d} Opens key: HKCU\software\classes\

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

08002b30309d}\inprocserver32

 $HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver 32$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\setupapi.dll

Opens key: HKLM\system\currentcontrolset\control\minint Opens key: HKLM\svstem\wpa\pnp

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

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

HKLM\software\microsoft\windows\currentversion\setup\apploglevels Opens key: Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\policies\microsoft\system\dnsclient

 ${\tt HKLM \backslash software \backslash microsoft \backslash rpc \backslash paged buffers}$ Opens key:

Opens key: HKLM\software\microsoft\rpc

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

options\71985e8a4de40ddc1151fafb929b5614.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername

Opens key:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-f9025fc2-$ 

11e3-9fc7-806d6172696f}\

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}

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

409d6c4515e9}

Opens key: HKCU\software\classes\directory

HKCR\directory Opens key:

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

Opens key: HKCR\directory\curver Opens key: HKCR\directorv\

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

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

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

Opens key: HKCR\directory\clsid

Opens key: HKCU\software\classes\folder

HKCR\folder Opens key:

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

Opens key: HKCR\folder\clsid

 $\label{lem:hklm} \mbox{HKLM} \mbox{$\tt M$} \mbox{$\tt M$}$ Opens key:

options\system.dll

Opens key: HKCU\software\appdatalow\software\smartbar HKCU\software\clients\startmenuinternet Opens key: Opens key: HKLM\software\clients\startmenuinternet

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

options\comdlg32.dll

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

options\winspool.drv

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

options\oledlg.dll

Opens key: HKCU\software\classes\clsid

Opens key: HKCR\clsid

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

options\oleaut32.dll

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

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

options\msasn1.dll

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

options\crypt32.dll

Opens key:  $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ crypt 32 \+ performance$ Opens key:  $HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash msasn1$ 

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcp60.dll

Opens key:

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

Opens key:

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\normaliz.dll

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 HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_protocol\_lockdown

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\ Opens key: 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 key: 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\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\ranges\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_unc\_savedfilecheck HKI M\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_unc\_savedfilecheck Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll Opens key: HKLM\system\currentcontrolset\control\wmi\security Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\webapphost.dll Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility 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:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ app compatflags\+ layers$ HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\bi.exe HKLM\software\policies\microsoft\windows\safer\levelobjects Opens key: Opens key: Opens key: be2efd2c1a33} Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: edd5fbde1328} Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91} Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f} Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d} Opens kev:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{dc971ee5-44eb-4fe4-ae2e-4fe4-ae2$ b91490411bfc} Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: 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\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key:  $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus has hes$ 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: 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\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\bi.exe Opens key: HKLM\software\microsoft\ctf\compatibility\bi.exe Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\bi.exe\rpcthreadpoolthrottle  $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows}\ nt\current\sc version\sc mage file execution}$ Opens key: options\inetc.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\imm Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime Opens kev: HKCU\software\microsoft\ctf HKLM\software\microsoft\ctf\systemshared Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies Opens key: HKCU\software\policies Opens key: HKCU\software HKLM\software Opens kev: Opens key: HKLM\software\policies\microsoft\internet explorer HKLM\software\policies\microsoft\internet explorer\main Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\content HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\cookies  $\label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet$ Opens key: settings\5.0\cache\cookies HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\history HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\history HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\extensible cache\domstore Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\ietld Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014041220140413

HKCU\software\microsoft\windows\currentversion\internet

Opens kev:

settings\5.0\cache\extensible cache\privacie:

```
HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                     HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                     HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                     HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                     HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                     HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                     HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                     HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                     HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                     HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                     HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                     HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens kev:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                     HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
 Opens key:
                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
                     HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens kev:
Opens key:
Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
 Opens key:
Opens kev:
```

```
Opens key:
```

Opens kev:

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000004

Opens key:

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

Opens kev:

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003

Opens kev: HKCU\software\microsoft\windows\currentversion\internet settings\wpad

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615

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

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version} \nointernet settings \http \end{tabular}$ Opens key:

filters\rpa

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

filters\rpa

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_mime\_handling Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_mime\_handling HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key: options\netapi32.dll

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

Opens key:

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

options\rtutils.dll

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

options\winmm.dll

HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key:

Opens key:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm

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

options\tapi32.dll

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

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

options\rasapi32.dll

HKLM\software\microsoft\tracing\rasapi32 Opens key:

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 Opens key:

Opens key: HKU\

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

1757981266-507921405-1957994488-1003 Opens key: HKCU\environment Opens key: HKCU\volatile environment

Opens key:  $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabul$ 

options\sensapi.dll

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

options\mswsock.dll

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

options\rasadhlp.dll

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

options\dnsapi.dll

Opens kev: HKLM\svstem\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\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:
```

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4304-a$ 

c7d49d7cecdc}

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

Opens key: HKLM\system\currentcontrolset\control\securityproviders
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache

Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msv1\_0.dll

Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider

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

options\asycfilt.dll

Opens key: HKLM\software\microsoft\com3

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

options\comres.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: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}

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

00c04fd705a2}\treatas

Opens key:  $\begin{tabular}{ll} HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-} \end{tabular}$ 

00c04fd705a2}\inprocserver32

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32

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

00c04fd705a2}\inprocserverx86

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86

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

00c04fd705a2}\localserver32

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32

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

00c04fd705a2}\inprochandler32

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32

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

00c04fd705a2}\inprochandlerx86

Opens key:  $\label{eq:hkcr_clsid} \begin{tabular}{ll} HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx 86. \end{tabular}$ 

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

00c04fd705a2}\localserver

Opens key:  $\label{eq:hkcr} \mbox{HKCR\clsid} \mbox{\{8856f961-340a-11d0-a96b-00c04fd705a2\}\localserver}$ 

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

options\ieframe.dll

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe

Opens key: HKLM\software\microsoft\internet explorer\setup

Opens key: HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-

0000c05bae0b}\typelib

Opens key: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-

00aa00404770}\proxystubclsid32

Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-

00aa004ba90b}\proxystubclsid32

Opens key: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{000214e6-0000-0000-c000-

 $000000000046 \} \\ \ proxystubcl sid 32$ 

 $Opens~key: \\ HKCR \ interface \\ \{000214e6-0000-0000-c000-00000000046\} \\ \ proxystubclsid 32 \\$ 

Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-

00c04f79abd1}\proxystubclsid32

Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32

Opens key: HKCU\software\microsoft\internet explorer\main

Opens key: HKCU\software\microsoft\internet explorer\searchscopes

Opens key: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-

472f-a0ff-e1416b8b2e3a}

Opens key: HKLM\software\microsoft\internet explorer\toolbar
Opens key: HKLM\software\microsoft\net framework setup\ndp

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\microsoft\internet explorer\main

Opens key: HKLM\software\microsoft\net framework setup\ndp\v2.0.50727
Opens key: HKLM\software\microsoft\net framework setup\ndp\v3.0
Opens key: HKCU\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\microsoft\net framework setup\ndp\v3.5
Opens key: HKLM\software\microsoft\windows nt\currentversion

```
Opens key:
```

a2ea-08002b30309d}

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32

Opens key: HKCU\software\conduit\distributionengine\1\offerhistory

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\treatas

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserverx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\localserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprochandler32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprochandlerx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\localserver

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_iedde\_register\_protocol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_iedde\_register\_protocol

Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\policies\microsoft\internet explorer\browseremulation
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rsaenh.dll

Opens key: HKCU\software\classes\protocols\name-space handler\res\

Opens key: HKCR\protocols\name-space handler\res

Opens key: HKCU\software\classes\protocols\name-space handler\\*\

Opens key: HKCR\protocols\name-space handler\\*

Opens key: HKCU\software\classes\protocols\handler\res

Opens key: HKCR\protocols\handler\res

 $Opens\ key: \\ HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f3bc-98b5-11cf-bb82-00aa00bdce0b\}$ 

 Opens key:
 HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}

 Opens key:
 HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82

00aa00bdce0b}\treatas

00aa00bdce0b}\inprocserver32

Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32

Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprocserverx86

Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\localserver32

Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32

Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCR} \\ \mathsf{Clsid} \\ \{3050f3bc-98b5-11cf-bb82-00aa00bdce0b\} \\ \mathsf{inprochandler32}$ 

Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprochandlerx86

Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\localserver

 $Opens~key: \\ HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver$ 

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

options\msls31.dll Opens key:

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

options\mshtml.dll

Opens key: HKCU\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature\_css\_data\_respects\_xss\_zone\_setting\_kb912120$ 

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_css\_data\_respects\_xss\_zone\_setting\_kb912120

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_aria\_support

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_aria\_support

 $\label{lem:constrain} Opens \ key: $$ HKCU\software\microsoft\internet explorer\main\feature\control\feature\_legacy\_dispparams$ 

Opens key: HKLM\software\microsoft\internet

```
HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_private_font_setting
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_css_show_hide_events
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_expanduri bypass
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enforce_bstr
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\windows
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_cleanup_at_fls
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
 Opens key:
                         HKLM\software\microsoft\internet explorer\application compatibility
                         HKLM\software\policies\microsoft\internet explorer\domstorage
 Opens key:
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\domstorage
 Opens kev:
                         HKCU\software\microsoft\internet explorer\domstorage
                         HKLM\software\microsoft\internet explorer\domstorage
 Opens key:
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\safety\privacie
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\safety\privacie
                         HKCU\software\microsoft\internet explorer\safety\privacie
 Opens key:
 Opens key:
                         HKLM\software\microsoft\internet explorer\safety\privacie
 Opens key:
                         HKLM\software\microsoft\internet explorer\mediatypeclass
                         HKLM\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\accepted documents
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\policies\ratings
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                         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\
 Opens key:
                         \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings\zonemap\domains\
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
```

explorer\main\featurecontrol\feature\_legacy\_dispparams

```
settings\zonemap\domains\msn.com
                           HKLM\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\domains\msn.com\related
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                          HKCU\software\microsoft\internet explorer\ietld
 Opens key:
                           HKLM\software\policies\microsoft\internet explorer\security
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
 Opens key:
                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet settings \setminus zones \setminus 1
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                           HKLM\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 key:
settings\zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 Opens key:
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
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
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\
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\0
 Opens key:
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\lockdown_zones\0
 Opens key:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
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:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
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
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\4
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
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

```
Opens key:
                        HKCU\software\microsoft\internet explorer
Opens key:
                        HKLM\software\microsoft\internet explorer
Opens kev:
                        HKLM\software\policies\microsoft\cryptography
Opens key:
                        HKLM\software\microsoft\cryptography
Opens kev:
                        HKLM\software\microsoft\cryptography\offload
Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
```

options\hnetcfg.dll

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_restrict\_res\_to\_lmz Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_restrict\_res\_to\_lmz HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_load\_shdoclc\_resources Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_load\_shdoclc\_resources Opens key: HKCU\software\classes\.htm

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

options\wshtcpip.dll

Opens key: HKCR\.htm

Opens key: HKCU\software\classes\protocols\filter\text/html

HKCR\protocols\filter\text/html Opens kev: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_mime\_sniffing HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_mime\_sniffing Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_safe\_bindtoobject

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_safe\_bindtoobject

HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} Opens key:

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\treatas

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserver32

Opens key:  $HKCR \c1sid \end{25336920-03f9-11cf-8fd0-00aa00686f13} \label{eq:hkcr} in proceser ver 32$ 

Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserverx86

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\localserver32

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32

Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprochandler32

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32

HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-Opens kev:

00aa00686f13}\inprochandlerx86

HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86 Opens kev:

HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-Opens key:

00aa00686f13}\localserver

 $\label{localserver} $HKCR\clsid{25336920-03f9-11cf-8fd0-00aa00686f13} \land calserver $$ $HKCR\clsid{25336920-03f9-00aa00686f13} \land calserver $$ $HKCR\clsid{25336920-03f9-00aa00686666} \land calserver $$ $HKCR\clsid{25336920-03f9-00aa0068666}$ Opens key:

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

options\psapi.dll

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature manage script circular refs HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_manage\_script\_circular\_refs Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_restrict\_filedownload HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_restrict\_filedownload

HKLM\software\microsoft\internet explorer\security\floppy access Opens key: Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof

detection

HKLM\software\microsoft\internet explorer\security\adv addrbar spoof Opens key:

detection

HKCU\software\classes\protocols\name-space handler\about\ Opens kev:

Opens key: HKCR\protocols\name-space handler\about Opens key: HKCU\software\classes\protocols\handler\about

Opens key: HKCR\protocols\handler\about

 $\label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \end{tabular}$ Opens key:

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\treatas

 $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas$ Opens kev: Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

Opens key:  $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\tinprocserver32$ 

HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprocserverx86

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\localserver32

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandlerx86

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\localserver

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_document\_compatible\_mode Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_document\_compatible\_mode

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3

Opens key: HKLM\software\policies\microsoft\internet explorer\zoom Opens key: HKCU\software\policies\microsoft\internet explorer\zoom

Opens key: HKCU\software\microsoft\internet explorer\zoom Opens key: HKLM\software\microsoft\internet explorer\zoom

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_weboc\_document\_zoom Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_weboc\_document\_zoom

Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\progid

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_enable\_compat\_logging Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_enable\_compat\_logging

Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\international

Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts

Opens key: HKCU\software\microsoft\internet explorer\international\scripts
Opens key: HKLM\software\microsoft\internet explorer\international\scripts
Opens key: HKLM\software\policies\microsoft\internet explorer\settings

Opens key: HKCU\software\microsoft\internet explorer\settings
Opens key: HKLM\software\microsoft\internet explorer\settings
Opens key: HKCU\software\microsoft\internet explorer\styles

 $Opens\ key: \\ HKCU\software\microsoft\windows\currentversion\policies\active desktop$ 

Opens key: HKCU\software\microsoft\windows\currentversion\policies
Opens key: HKCU\software\microsoft\internet explorer\pagesetup
Opens key: HKCU\software\microsoft\internet explorer\menuext
Opens key: HKCU\software\microsoft\internet explorer\menuext\%s
Opens key: HKLM\system\currentcontrol\set\control\nls\codepage

Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mlang.dll

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

Opens key: HKLM\software\microsoft\internet explorer\version vector

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_zslux

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_sslux

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_xssfilter

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_xssfilter

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_shim\_mshelp\_combine Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_shim\_mshelp\_combine Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_subdownload\_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_subdownload\_lockdown Opens key: HKCU\software\classes\.css

Opens key: HKCR\.css

Opens key:  $\label{local-constraints} \mbox{HKCU\software\classes\protocols\filter\text/css}$ 

Opens key: HKCR\protocols\filter\text/css
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_custom\_image\_mime\_types\_kb910561

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_custom\_image\_mime\_types\_kb910561

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation| \\$ 

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_behaviors

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_behaviors

Opens key: HKLM\software\microsoft\internet explorer\default behaviors
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}

 Opens key:
 HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}

 Opens key:
 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82

00aa00bdce0b}\treatas

00aa00bdce0b}\inprocserver32

Opens key:  $\label{eq:hkcr} \mbox{HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\windows{1000} \mbox{hinprocserver32} \mbox{ } \mbox{$ 

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprocserverx86

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\localserver32

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprochandlerx86

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\localserver

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver

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

options\iepeers.dll

Opens key: HKCU\software\policies\microsoft\internet explorer\persistence Opens key: HKLM\software\policies\microsoft\internet explorer\persistence

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_binary\_caller\_service\_provider

Opens key: HKLM\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature\_binary\_caller\_service\_provider$ 

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

Opens key: HKCU\software\microsoft\internet explorer\dxtrans
Opens key: HKLM\software\microsoft\internet explorer\dxtrans

Opens key: HKCU\software\classes\.js

Opens key: HKCR\.js

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_feeds| \\$ 

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_feeds

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_block\_lmz\_script Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_block\_lmz\_script

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

settings\

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

settings\zonemap\

 $Opens~key: \\ HKCU \ software \ policies \ microsoft \ windows \ current version \ internet$ 

settings\zonemap\

Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\treatas

f4ceaaf59cfc}\inprocserver32

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32

Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\inprocserverx86

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\localserver32

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32

Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-

```
f4ceaaf59cfc}\inprochandler32
                                                                                                         HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
      Opens kev:
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandlerx86
      Opens kev:
                                                                                                         HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
      Opens key:
                                                                                                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d
f4ceaaf59cfc}\localserver
      Opens key:
                                                                                                        HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver
      Opens key:
                                                                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimtf.dll
      Opens kev:
                                                                                                         HKLM\software\microsoft\ctf\tip
      Opens key:
                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\languageprofile
                                                                                                        HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
      Opens key:
c9633f71be64}\languageprofile
      Opens key:
                                                                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000
      Opens key:
                                                                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
                                                                                                        \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \ \{3ce74de4-53d3-4d74-8b83-431b3828ba53\} \end{tabular}
      Opens key:
      Opens key:
                                                                                                         HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\treatas
      Opens key:
                                                                                                         HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32
                                                                                                         HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
      Opens key:
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserverx86
      Opens key:
                                                                                                         HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver32
                                                                                                         HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
      Opens key:
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandler32
      Opens key:
                                                                                                         HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandlerx86
                                                                                                         HKCR \c1sid \c2seq4de4-53d3-4d74-8b83-431b3828ba53 \c2seq4de4-53d3-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-8d74-8b83-8d74-8b83-8d74-8b83-8d74-8b83-8d74-8b83-8d74-8
      Opens key:
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver
      Opens key:
                                                                                                         HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
                                                                                                         HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
      Opens kev:
                                                                                                         HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
      Opens key:
869523e2d6c7}\treatas
                                                                                                         HKCR\clsid{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
      Opens key:
      Opens key:
                                                                                                         869523e2d6c7}\inprocserver32
                                                                                                        Opens key:
                                                                                                         HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
      Opens kev:
869523e2d6c7}\inprocserverx86
                                                                                                         HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
      Opens key:
869523e2d6c7}\localserver32
                                                                                                        HKCR \ clsid \ \{a4b544a1-438d-4b41-9325-869523e2d6c7\} \ localserver 32
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
      Opens key:
869523e2d6c7}\inprochandler32
                                                                                                         HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
      Opens key:
      Opens key:
                                                                                                         HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandlerx86
      Opens key:
                                                                                                        HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
                                                                                                         HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
      Opens key:
869523e2d6c7}\localserver
                                                                                                        HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
      Opens key:
      Opens key:
                                                                                                         HKLM\software\microsoft\ctf\tip\
      Opens key:
                                                                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
{\tt c9633f71be64} \\ {\tt category} \\ {\tt b95f181b-ea4c-4af1-8056-7c321abbb091} \\ {\tt c9633f71be64} \\ {\tt category} \\ {
      Opens key:
                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
      Opens key:
                                                                                                         HKLM \setminus software \setminus icrosoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-b4b4\} = \{c1ee01f2-b3b6-4a6a-9ddb-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b4b6-6ab4\} 
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                        HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
      Opens kev:
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
      Opens key:
                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2
Of816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
      Opens key:
                                                                                                         HKCU\software\microsoft\ctf\langbaraddin\
                                                                                                         HKLM\software\microsoft\ctf\langbaraddin\
      Opens kev:
      Opens key:
                                                                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
```

HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = \{c1ee01f2-b3b6-4a6a-9ddb-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a$ 

77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}

Opens key:

Opens key:

```
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                    HKLM \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143
     Opens key:
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                     HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
     Opens key:
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
     Opens key:
                                                                    HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
 c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Opens key:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
     Opens key:
                                                                     HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
     Opens key:
                                                                     HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                    HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
    Opens key:
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
     Opens key:
                                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
Opens key:
                                                                     HKCU\software\policies\microsoft\internet explorer\control panel
     Opens key:
                                                                     HKCU\software\microsoft\windows\currentversion\internet settings\url
history
     Opens key:
                                                                    HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_iedde_register_urlecho
     Opens kev:
                                                                    HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_iedde_register_urlecho
     Opens key:
                                                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
                                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
     Opens key:
     Opens key:
                                                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
                                                                     HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
     Opens kev:
     Opens key:
                                                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
                                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
     Opens key:
     Opens key:
                                                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserverx86
     Opens key:
                                                                    Opens key:
                                                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver32
                                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
     Opens key:
     Opens key:
                                                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
                                                                    HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprochandler32
     Opens key:
     Opens key:
                                                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandlerx86
                                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
     Opens key:
     Opens key:
                                                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver
                                                                    HKCR \ clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \ local server
     Opens key:
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jscript.dll
     Opens key:
                                                                     HKLM\software\microsoft\windows script\features
                                                                     HKCU\software\microsoft\internet
     Opens kev:
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
     Opens key:
                                                                    HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
     Opens kev:
                                                                    HKLM\software\microsoft\internet explorer\activex compatibility
     Opens key:
                                                                    HKLM\software\microsoft\internet explorer\activex
 compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
     Opens key:
                                                                    HKLM\system\currentcontrolset\control\nls\locale
     Opens key:
                                                                    HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
     Opens key:
                                                                     HKLM\system\currentcontrolset\control\nls\language groups
     Opens key:
                                                                     HKCU\software\classes\appid\71985e8a4de40ddc1151fafb929b5614.exe
     Opens key:
                                                                     HKCR \land ppid \land 71985e8a4de40ddc1151fafb929b5614.exe
     Opens key:
                                                                     HKLM\system\currentcontrolset\control\lsa
     Opens key:
                                                                    HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_scripturl_mitigation
     Opens key:
                                                                    HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_scripturl_mitigation
     Opens key:
                                                                    HKCU\software\classes\.jpg
     Opens key:
                                                                     HKCR\.jpg
                                                                     HKCU\software\classes\protocols\filter\image/jpeg
     Opens key:
     Opens key:
                                                                     HKCR\protocols\filter\image/jpeg
     Opens key:
                                                                     HKCU\software\classes\.png
     Opens key:
                                                                     HKCR\.png
                                                                     HKCU\software\classes\protocols\filter\image/png
     Opens key:
     Opens key:
                                                                     HKCR\protocols\filter\image/png
     Opens key:
                                                                    HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_block_lmz_img
                                                                    HKLM\software\microsoft\internet
     Opens key:
 explorer\main\featurecontrol\feature_block_lmz_img
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imgutil.dll
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
```

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01} Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01} Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas Opens kev: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas Opens key: 00aa006c1a01}\inprocserver32 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86 Opens kev: Opens key: 00aa006c1a01}\localserver32 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32 Opens key: Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\\inprochandler32 Opens kev: Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86 Opens key: Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver Opens kev: Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key: 00aa006c1a01}\treatas Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key:

00aa006c1a01}\inprocserver32

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\inprocserverx86

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

 $00aa006c1a01 \} \\ local server 32$ 

 $Opens~key: \\ HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver 32$ 

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\inprochandler32

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\inprochandlerx86

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\localserver

 $Opens~key: \\ \qquad \qquad \text{HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\localserver} \\$ 

Opens key: HKCU\software\classes\mime\database\content type

Opens key: HKCR\mime\database\content type

Opens key: HKCU\software\classes\mime\database\content type\image/bmp\bits

Opens key: HKCR\mime\database\content type\image/bmp\bits
Opens key: HKCU\software\classes\mime\database\content type\image/gif\bits

Opens key: HKCO\software\classes\mime\database\content type\image/gif\bits

Opens key: HKCR\mime\database\content type\image/gif\bits

Opens key: HKCU\software\classes\mime\database\content type\image/jpeg\bits

Opens key: HKCR\mime\database\content type\image/jpeg\bits

Opens key: HKCU\software\classes\mime\database\content type\image/pjpeg\bits

Opens key: HKCR\mime\database\content type\image/pjpeg\bits

Opens key: HKCU\software\classes\mime\database\content type\image/png\bits

Opens key: HKCR\mime\database\content type\image/png\bits

Opens key. HKCK\IIIIIlle \uacabase \content type \tiliage/pig\bits

Opens key: HKCU\software\classes\mime\database\content type\image/tiff\bits

Opens key: HKCR\mime\database\content type\image/tiff\bits

Opens key: HKCU\software\classes\mime\database\content type\image/x-icon\bits

Opens key: HKCR\mime\database\content type\image/x-icon\bits

Opens key: HKCU\software\classes\mime\database\content type\image/x-jg\bits

Opens key:  ${\tt HKCR\mime\database\content\ type\image/x-jg\bits}$ 

Opens key: HKCU\software\classes\mime\database\content type\image/x-png\bits

Opens key:  ${\sf HKCR} \\ {\sf mime} \\ {\sf database} \\ {\sf content type} \\ {\sf image} \\ {\sf x-png} \\ {\sf bits} \\$ 

Opens key: HKCU\software\classes\mime\database\content type\image/x-wmf\bits

Opens key: HKCR\mime\database\content type\image/x-wmf\bits

Opens key: HKCU\software\classes\mime\database\content type\image/x-png

Opens key: HKCR\mime\database\content type\image/x-png

 $Opens~key: \\ HKCU \setminus software \setminus (a3ccedf7-2de2-11d0-86f4-00a0c913f750) \\$ 

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750} Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\treatas

00a0c913f750}\inprocserver32

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprocserverx86

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\localserver32

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprochandler32

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprochandlerx86

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\localserver

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver

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

options\pngfilt.dll

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

Opens key: HKCU\software\microsoft\internet explorer\recovery
Opens key: HKLM\software\microsoft\internet explorer\recovery

Opens key: HKCU\software\microsoft\ftp

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

Opens key: HKCU\software\microsoft\internet explorer\services
Opens key: HKLM\software\microsoft\internet explorer\services

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

Opens key: HKCU\software\microsoft\internet explorer\activities
Opens key: HKLM\software\microsoft\internet explorer\activities

Opens key:  $\mbox{HKLM\software\policies\mbox{\sc microsoft\internet}}$ 

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites

Opens key: HKCU\software\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\microsoft\internet explorer\feed discovery

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_isolate\_named\_windows Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_isolate\_named\_windows

Opens key: HKCU\software\classes\protocols\name-space handler\http\

Opens key: HKCR\protocols\name-space handler\http

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

HKCU\software\microsoft\windows\currentversion\internet

agent

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent

Opens key:

settings\5.0\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\user agent

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

agent\ua tokens

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

agent\pre platform

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\user agent\pre platform

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

agent\post platform

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

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_maxconnectionsperserver Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_maxconnectionsperserver Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_maxconnectionsper1\_0server Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature maxconnectionsper1\_0server

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_legacy\_compression Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_legacy\_compression

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\treatas

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserver32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserverx86

Opens key:  $\label{eq:hkcr} \mbox{HKCR\clsid\efo9bde7-a8dc-47f3-893f-fd2b31b3eefd} \mbox{\clsid\efo9bde7-a8dc-47f3-893f-fd2b31b3eefd} \mbox{\clsid\efo9bde7-a8$ 

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\localserver32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver32

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandler32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandlerx86

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\localserver

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_additional\_ie8\_memory\_cleanup

Opens key: HKLM\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature\_additional\_ie8\_memory\_cleanup| \\$ 

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_navigation\_sounds

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_navigation\_sounds

Opens key: HKCU\appevents\schemes\apps\explorer\activatingdocument\.current
Opens key: HKCU\software\microsoft\internet explorer\searchproviders\

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_activex\_inactivate\_mode\_removal\_revert

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_activex\_inactivate\_mode\_removal\_revert

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

options\xml.dll

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

options\nsarray.dll

Opens key: HKLM\system\currentcontrolset\control\windows

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

Opens key: HKCU\software\classes\htmlfile

Opens key: HKCR\htmlfile

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

Opens key: HKCR\htmlfile\curver
Opens key: HKCR\htmlfile\

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

Opens key: HKCR\htmlfile\shellex\iconhandler

Opens key: HKCU\software\classes\systemfileassociations\.htm

Opens key: HKCR\systemfileassociations\.htm

Opens key: HKCU\software\classes\systemfileassociations\text

 $\begin{tabular}{lll} Opens~key: & HKCR\systemfileassociations \text \\ Opens~key: & HKCU\software\classes \tmlfile\clsid \end{tabular}$ 

Opens key: HKCR\htmlfile\clsid

Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented categories\{00021490-0000-0000-c000-00000000046}

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented

categories\{00021490-0000-0000-c000-00000000046}

Opens key:  $\label{local-opens} \mbox{ HKCU\appevents\schemes\apps\explorer\navigating\.current } \mbox{ } \mb$ 

Opens key: HKCU\software\microsoft\multimedia\sound mapper
Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap
Opens key: HKCU\software\classes\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-

13914bef5890}

 Opens key:
 HKCR\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}

 Opens key:
 HKCU\software\classes\.htm\shellex\{a39ee748-6a27-4817-a6f2

13914bef5890}

Opens key: HKCR\.htm\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}

Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{a39ee748-

6a27-4817-a6f2-13914bef5890}

Opens key: HKCR\systemfileassociations\text\shellex\{a39ee748-6a27-4817-a6f2-

13914bef5890}

Opens key: HKCU\software\classes\\*

Opens key: HKCR\

 $Opens~key: \\ HKCU \setminus software \setminus \{a39ee748-6a27-4817-a6f2-13914bef5890\}$ 

Opens key: HKCR\\*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}

Opens key: HKCU\software\classes\htmlfile\shellex\{000214e6-0000-0000-c000-

000000000046}

000000000046}

Opens key: HKCR\.htm\shellex\{000214e6-0000-0000-c000-00000000046}

Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{000214e6-

0000-0000-c000-000000000046}

Opens key: HKCR\systemfileassociations\text\shellex\{000214e6-0000-0000-c000-

000000000046}

Opens key: HKCU\software\classes\\*\shellex\{000214e6-0000-0000-c000-00000000046}

Opens key: HKCR\\*\shellex\{000214e6-0000-0000-c000-00000000046}
Opens key: HKCU\software\classes\protocols\name-space handler\file\

Opens key: HKCR\protocols\name-space handler\file
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_ignore\_leading\_file\_separator\_in\_uri\_kb933105

Opens key: HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105
   Opens key:
                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_crossdomain_fix_kb867801
    Opens key:
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_crossdomain_fix_kb867801
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
                                                       HKCU\software\microsoft\windows\currentversion\thememanager
    Opens key:
    Opens key:
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
    Opens key:
    Opens key:
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\treatas
    Opens key:
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
                                                       Opens key:
00aa003f8646}\inprocserver32
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
    Opens key:
    Opens kev:
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserverx86
    Opens key:
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserverx86
    Opens key:
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\localserver32
    Opens key:
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver32
    Opens kev:
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler32
    Opens key:
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler 32
    Opens key:
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandlerx86
    Opens key:
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandlerx86
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
    Opens kev:
00aa003f8646}\localserver
    Opens key:
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\}
    Opens key:
    Opens key:
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
    Opens key:
                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell
                                                       HKCR \ clsid \ \{ff393560-c2a7-11cf-bff4-444553540000\} \ shell
    Opens key:
                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
    Opens key:
444553540000}\shellex\iconhandler
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellex\iconhandler
    Opens key:
    Opens key:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560-c2a7-11cf-bff4-444553540000\} \setminus clsid \setminus ff393560-c2a7-11cf-bff4-444553540000\} \setminus clsid \setminus ff393560-c2a7-11cf-bff4-444553540000\}
    Opens key:
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid
    Opens key:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c
444553540000}\inprocserver32
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
    Opens kev:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c
    Opens key:
444553540000}\treatas
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
    Opens key:
    Opens key:
                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserverx86
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserverx86
    Opens kev:
    Opens key:
                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\localserver32
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32
    Opens key:
    Opens key:
                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler32
    Opens kev:
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
    Opens key:
                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandlerx86
    Opens key:
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandlerx86
    Opens key:
                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\localserver
    Opens key:
                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver
    Opens key:
bff4-444553540000}
                                                       HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\5.0\cache\extensible cache\mshist012016042820160429
    Opens key:
                                                       HKCU\software\microsoft\internet explorer\main\windowssearch
                                                       HKLM\software\policies\microsoft\internet explorer\feeds
    Opens key:
    Opens key:
                                                       HKCU\software\microsoft\internet explorer\feeds
    Opens key:
                                                       HKLM\software\microsoft\internet explorer\feeds
    Opens key:
                                                       HKCU\software\classes\.url\persistenthandler
```

Opens key: HKCR\.url\persistenthandler

Opens key: HKLM\software\policies\microsoft\internet explorer\main\windowssearch

Opens key: HKLM\software\microsoft\windows search

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

08002b30309d\shellfolder

 $Opens~key: \\ HKCU software \verb|microsoft| windows \verb|currentversion| explorer \verb|clsid| \{20d04feo-defined by the context of the$ 

3aea-1069-a2d8-08002b30309d}

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

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

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

```
Opens key:
                                                         HKLM \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-delta \ explorer \ ex
3aea-1069-a2d8-08002b30309d}\shellfolder
                                                         \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \ \{20d04fe0-3aea-1069-a2d8-08002b30309d\} \end{tabular}
    Opens kev:
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
    Opens key:
    Opens key:
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\
    Opens key:
                                                         {\tt HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam}
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\muicache
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\muicache\
    Opens key:
                                                         c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Opens kev:
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
    Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-14d}
00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                         HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
    Opens kev:
Of816c09f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
    Queries value:
                                                         HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Oueries value:
                                                         HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                         HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                                         HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\compatibility32[71985e8a4de40ddc1151fafb929b5614]
                                                         HKLM\software\microsoft\windows nt\currentversion\ime
    Queries value:
compatibility[71985e8a4de40ddc1151fafb929b5614]
                                                         HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
    Oueries value:
    Queries value:
                                                         HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
    Queries value:
                                                         HKLM\system\setup[systemsetupinprogress]
    Queries value:
                                                         HKCU\control panel\desktop[multiuilanguageid]
    Queries value:
                                                         HKCU\control panel\desktop[smoothscroll]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
                                                         HKLM\system\currentcontrolset\control\session
    Queries value:
manager[criticalsectiontimeout]
                                                         HKLM\software\microsoft\ole[rwlockresourcetimeout]
    Oueries value:
    Queries value:
                                                         HKCR\interface[interfacehelperdisableall]
    Queries value:
                                                         HKCR\interface[interfacehelperdisableallforole32]
                                                         HKCR\interface[interfacehelperdisabletypelib]
    Oueries value:
                                                         HKCR\interface\{00020400-0000-0000-c000-
    Queries value:
00000000046}[interfacehelperdisableall]
                                                         HKCR\interface\{00020400-0000-0000-c000-
    Queries value:
00000000046}[interfacehelperdisableallforole32]
    Queries value:
                                                         HKLM\software\microsoft\ctf\systemshared[cuas]
    Oueries value:
                                                         HKCU\keyboard layout\toggle[language hotkey]
    Queries value:
                                                         HKCU\keyboard layout\toggle[hotkey]
    Oueries value:
                                                         HKCU\keyboard layout\toggle[layout hotkey]
    Queries value:
                                                         HKLM\software\microsoft\ctf[enableanchorcontext]
    Oueries value:
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]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
    Queries value:
                                                         HKLM\system\wpa\pnp[seed]
    Oueries value:
    Oueries value:
                                                         HKLM\system\setup[osloaderpath]
                                                         HKLM\system\setup[systempartition]
    Oueries value:
    Queries value:
                                                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} Software \end{tabular} in the local hammon \end{tabular} and the local hammon \end{tabular} in the local hammon \end{tabular} and \end{tabular} and \end{tabular} in the local hammon \end{tabular} and \end
    Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
                                                         HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
    Oueries value:
    Oueries value:
                                                         HKLM\software\microsoft\windows\currentversion[devicepath]
    Queries value:
                                                         HKLM\software\microsoft\windows\currentversion\setup[loglevel]
    Queries value:
                                                         HKLM\software\microsoft\windows\currentversion\setup[logpath]
    Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                                         HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
    Oueries value:
    Oueries value:
                                                         HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
    Oueries value:
                                                         HKLM\software\microsoft\rpc[maxrpcsize]
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-6bc4-f9025fc2-
```

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[data]

Oueries value:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-five \ for \$ 11e3-9fc7-806d6172696f}[generation] Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon] Oueries 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] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Queries value:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced \ [dont pretty path]$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Queries value:  $HKCU \ software \ `microsoft \ `windows \ `current version \ `explorer \ `advanced \ [mapnet drvbtn]" \ in the context of th$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] HKCR\directory[docobject] Oueries value: HKCR\directory[browseinplace] Queries value: Queries value: HKCR\directory[isshortcut] Queries value: HKCR\directory[alwaysshowext] Oueries value: HKCR\directory[nevershowext] Queries value: HKLM\software\clients\startmenuinternet[]  $\label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet$ Oueries value: settings[disableimprovedzonecheck] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown[71985e8a4de40ddc1151fafb929b5614.exe] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature\_protocol\_lockdown[\*] Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45ab78-1084642581fb1 Oueries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000] Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode] Queries value:

 ${\tt HKLM \ } system \verb|\ current control \ session$ 

manager\appcompatibility[disableappcompat]

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

Oueries value:

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

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

Queries value:

be2efd2c1a33}[itemdata]

Oueries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths \setminus \{dda3f824 - d8cb - 441b - 834d - d8cb - 441b - 441$ be2efd2c1a33}[saferflags]

Queries value:

edd5fbde1328}[itemdata]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-4666f-9b89-46666$ edd5fbde1328}[hashalg1

Queries value:

edd5fbde1328}[itemsize]

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-4fe4-ae2e-4fe4-ae2$ b91490411bfc}[itemdata]

Oueries value:

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

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-4fe4-ae2e-4fe4-ae2$ b91490411bfc}[itemsize]

Oueries value:

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

Oueries value:

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

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [policy scope]$ 

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

folders[cache] Oueries value:

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

HKLM\software\microsoft\windows nt\currentversion\compatibility32[bi] Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[bi] Queries value:

Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown[bi.exe]

HKLM\software\microsoft\windows nt\currentversion\imm[ime file] Oueries value: Queries value: HKCU\software\microsoft\ctf[disable thread input manager] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings[fromcachetimeout]

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

settings[secureprotocols]

HKLM\software\policies\microsoft\internet Oueries value:

explorer\main[security\_hklm\_only]

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Oueries value: settings[certificaterevocation]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[disablekeepalive]

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

settings[disablepassport]

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

settings[idnenabled]

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

settings[cachemode]

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

settings[enablehttp1\_1]

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablebasicoverclearchannel]
 Queries value:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[signature]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[peruseritem]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[peruseritem]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[cache]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[peruseritem]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[cookies]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[peruseritem]
 Queries value:
                          \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings\5.0\cache\history[peruseritem]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[history]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Queries value:
                          settings\5.0\cache\extensible cache\iecompat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
```

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

Queries value:

```
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
 Queries value:
settings[disableworkerthreadhibernation]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[maxconnectionsper1_0server]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[certcachenovalidate]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[httpdefaultexpirytimesecs]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                            HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[bi.exe]
                            HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature disable unicode handle closing callback[*]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings[disablecachingofsslpages]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablent4rascheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendextracrlf]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypassftptimecheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduringauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[releasesocketduring401auth]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Queries value:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[disablelegacypreauthasserver]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sharecredswithwinhttp]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[mimeexclusionlistforcache]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[headerexclusionlistforcache]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[dnscacheentries]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonpost]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[warnalwaysonpost]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[warnonzonecrossing]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertsending]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[warnonbadcertrecving]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

settings[warnonpostredirect]

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

settings[alwaysdrainonredirect]

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

settings[warnonhttpstohttpredirect]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num]
Oueries value:

Queries value

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9 [next\_catalog\_entry\_id]$ 

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000001[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\0000000000002[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003[packedcatalogitem] Queries value:

 $HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog 9 \catalog\_entries \noon 000000000004 \packed catalog item] \\ Queries value:$ 

 $HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog 9 \catalog\_entries \noon 00000000005 \[packed catalog item] \queries value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007[packedcatalogitem]

Queries value:

 $\label{lem:hklmsystem} Hklm\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\0000000000008[packedcatalogitem] \\ Queries\ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000011[packedcatalogitem]

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\000000000001[librarypath]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring] Oueries 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]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
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\000000000002[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[displaystring]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[supportednamespace]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
Queries 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]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000003[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]

Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[storesserviceclassinfo] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32spincount] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enableautodial] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[urlencoding] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[truncatefilename]

HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[badproxyexpirestime] Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature mime handling[bi.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_mime\_handling[\*]

HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 4]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9] Queries value:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31 Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Oueries value: Oueries value:

HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]

Queries value:

Queries value:  ${\tt HKLM \setminus software \setminus microsoft \setminus tracing[enable consolet racing]}$ HKLM\software\microsoft\tracing\rasapi32[enablefiletracing] Oueries value: Queries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask] HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing] Oueries value: Oueries value: HKLM\software\microsoft\tracing\rasapi32[consoletracingmask] Queries value: HKLM\software\microsoft\tracing\rasapi32[maxfilesize] Queries value: HKLM\software\microsoft\tracing\rasapi32[filedirectory]

Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders[common appdata]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[userenvdebuglevel]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[chkaccdebuglevel]

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

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

folders[local settings]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[profilesdirectory]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[allusersprofile]

HKLM\software\microsoft\windows Oueries value: nt\currentversion\profilelist[defaultuserprofile]

Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] Oueries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003[profileimagepath] HKCU\software\microsoft\windows Oueries value:

nt\currentversion\winlogon[parseautoexec]

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

folders[appdata]

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

settings[migrateproxy]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

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

Queries value:

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

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[71985e8a4de40ddc1151fafb929b5614.exe]

Queries value:

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

Queries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ 

Queries value:

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

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries 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]

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

Oueries value:

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

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

Oueries value:

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

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

Queries value:

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: Queries 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] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]$ HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] c7d49d7cecdc}[enabledhcp] Queries value:  $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[leaseobtainedtime] Oueries value: c7d49d7cecdc}[leaseterminatestime] Queries value: c7d49d7cecdc}[dhcpserver] HKLM\software\microsoft\rpc\securityservice[10] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\securityproviders[securityproviders] HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name] Queries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid] HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]  $\label{thm:local_hamma} \begin{tabular}{ll} HKLM\system\currentcontrolset\control\space{0.05cm} Lisa\sspicache\digest.dll[name] \\ \end{tabular}$ Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] Queries value:

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]

HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize] Queries 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: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationmaxaddresscount] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[maxnumberofaddressestoregister] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[domain] Queries value: c7d49d7cecdc}[dhcpdomain] Queries value: c7d49d7cecdc}[ipautoconfigurationenabled] c7d49d7cecdc}[addresstype] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[nameserver] Queries value: c7d49d7cecdc}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Queries value:  $\label{lem:hklm} \verb+KLM\+ system \verb+ current control set \verb+ services \verb+ tcpip \verb+ parameters [dnsnbtlook upor der] + \texttt{look} +$ HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Oueries value: cryptographic provider[type]  $HKLM \ software \ \verb|microsoft| cryptography \ defaults \ \verb|provider| microsoft| strong$ Queries value: cryptographic provider[image path] HKLM\software\microsoft\com3[com+enabled] Oueries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess] Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject] Oueries value: HKLM\software\microsoft\com3[regdbversion] Oueries value: Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[inprocserver32] Oueries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]  $HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2\}[appid]$ Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-Oueries value: 00c04fd705a2}\inprocserver32[threadingmodel] HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[] Oueries value: Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow] Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedhigh] HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[] Queries value: Queries value: HKLM\software\microsoft\internet explorer\setup[installstarted] Oueries value: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[] Queries value: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[] Queries value: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]  $HKCR \land eface \land \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \land proxystubclsid32[]$ Queries value: Queries value:  $\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+shell$ folders[local appdata] Queries value: HKCU\software\microsoft\internet explorer\main[start page] HKCU\software\microsoft\internet explorer\searchscopes[defaultscope] Oueries value: Oueries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[url] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enablepunycode]

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

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

Queries value:

settings[enablepunycode]

```
HKLM\software\microsoft\internet explorer\main[navigationdelay]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[frametabwindow]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\internet explorer\main[frametabwindow]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[framemerging]
 Queries value:
                          HKLM\software\microsoft\net framework setup\ndp\v2.0.50727[install]
                          HKLM\software\microsoft\net framework setup\ndp\v2.0.50727[sp]
 Oueries value:
                          HKLM\software\microsoft\net framework setup\ndp\v3.0[install]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\net framework setup\ndp\v3.0[sp]
                          HKLM\software\microsoft\internet explorer\main[framemerging]
 Oueries value:
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[sessionmerging]
 Queries value:
                          HKLM\software\microsoft\internet explorer\main[sessionmerging]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[admintabprocs]
 Oueries value:
                          HKLM\software\microsoft\internet explorer\main[admintabprocs]
 Oueries value:
                          HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
                          HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
 Queries value:
                          HKLM\software\microsoft\net framework setup\ndp\v3.5[install]
 Oueries value:
                          HKLM\software\microsoft\net framework setup\ndp\v3.5[sp]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion[currentversion]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion[currentversion]
 Queries value:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
 Oueries value:
08002b30309d}\inprocserver32[loadwithoutcom]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x401]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x401]
 Queries value:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
 Queries value:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_handling[71985e8a4de40ddc1151fafb929b5614.exe]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
 Queries value:
                          HKCR\protocols\handler\res[clsid]
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
 Oueries value:
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[appid]
 Queries value:
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[71985e8a4de40ddc1151fafb929b5614.exe]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[71985e8a4de40ddc1151fafb929b5614.exe]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
 Queries value:
                          HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
 Oueries value:
                          HKLM\software\microsoft\internet explorer\application
compatibility[71985e8a4de40ddc1151fafb929b5614.exe]
 Queries value:
                          HKCU\software\microsoft\internet explorer\domstorage[totallimit]
 Queries value:
                          HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
 Queries value:
                          HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
 Queries value:
                          HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
 Queries value:
                          HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\zones\2[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[flags]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\zones\4[flags]
 Queries value:
                          HKCU\software\microsoft\internet
```

manager\environment[processor\_architecture]

```
explorer\main\featurecontrol\feature_localmachine_lockdown[71985e8a4de40ddc1151fafb929b5614.exe]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[71985e8a4de40ddc1151fafb929b5614.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[specialfolderscachesize]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
 Queries value:
                          HKCU\software\microsoft\internet explorer[no3dborder]
 Oueries value:
                          HKLM\software\microsoft\internet explorer[no3dborder]
                          HKLM\software\microsoft\cryptography[machineguid]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Queries value:
                          HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]
 Queries 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]
                          HKCR\.htm[content type]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[71985e8a4de40ddc1151fafb929b5614.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[istextplainhonored]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[71985e8a4de40ddc1151fafb929b5614.exe]
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-
 Oueries value:
00aa00686f13}\inprocserver32[inprocserver32]
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
 Oueries value:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-
 Queries value:
00aa00686f13}\inprocserver32[threadingmodel]
                         HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\windows[dragscrollinset]
                         HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\windows[dragscrolldelay]
 Queries value:
                         HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[71985e8a4de40ddc1151fafb929b5614.exe]
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_restrict_filedownload[*]
                         HKCR\protocols\handler\about[clsid]
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]
 Oueries value:
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[2106]
                          HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
 Queries value:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
 Oueries value:
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Oueries value:
                          HKCU\software\microsoft\internet explorer[smartdithering]
 Queries value:
                          HKCU\software\microsoft\internet explorer[rtfconverterflags]
                          HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[usecleartype]
                          HKLM\software\policies\microsoft\internet
explorer\main[page_transitions]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[page_transitions]
 Queries value:
                         HKLM\software\policies\microsoft\internet
explorer\main[use_dlgbox_colors]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
                          HKLM\software\policies\microsoft\internet explorer\main[anchor
 Oueries value:
underline1
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[anchor underline]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[css_compat]
                          HKCU\software\microsoft\internet explorer\main[expand alt text]
 Oueries value:
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer\main[display inline
```

images]

Queries value: HKCU\software\microsoft\internet explorer\main[display inline images]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline]

videos]

Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos]

Queries value: HKLM\software\policies\microsoft\internet

explorer\main[play\_background\_sounds]

Queries value: HKCU\software\microsoft\internet explorer\main[play\_background\_sounds] 
Queries value: HKLM\software\policies\microsoft\internet explorer\main[play\_animations]

Queries value: HKCU\software\microsoft\internet explorer\main[play\_animations]

Queries value: HKLM\software\policies\microsoft\internet

explorer\main[print\_background]

Queries value: HKCU\software\microsoft\internet explorer\main[print\_background]
Queries value: HKCU\software\microsoft\internet explorer\main[use stylesheets]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll]
Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[xmlhttp]
Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp]
Queries value: HKCU\software\microsoft\internet explorer\main[show image

placeholders]

Queries value: HKCU\software\microsoft\internet explorer\main[show image placeholders]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[disable script]

debugger]

Queries value:HKCU\software\microsoft\internetexplorer\main[disable script debugger]Queries value:HKCU\software\microsoft\internetexplorer\main[disablescriptdebuggerie]Queries value:HKCU\software\microsoft\internetexplorer\main[move system caret]Queries value:HKCU\software\microsoft\internetexplorer\main[force offscreen

composition]

Queries value: HKLM\software\policies\microsoft\internet explorer\main[enable

autoimageresize]

Queries value: HKCU\software\microsoft\internet explorer\main[enable autoimageresize]

Queries value: HKCU\software\microsoft\internet explorer\main[usethemes]
Queries value: HKCU\software\microsoft\internet explorer\main[useth]
Queries value: HKCU\software\microsoft\internet explorer\main[q300829]
Queries value: HKCU\software\microsoft\internet explorer\main[cleanup htcs]

Queries value: HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]

 Queries value:
 HKCU\software\microsoft\internet explorer\main[xdomainrequest]

 Queries value:
 HKLM\software\microsoft\internet explorer\main[xdomainrequest]

 Queries value:
 HKLM\software\policies\microsoft\internet explorer\main[domstorage]

Queries value: HKCU\software\microsoft\internet explorer\main[domstorage] Queries value: HKLM\software\microsoft\internet explorer\main[domstorage]

Queries value: HKCU\software\microsoft\internet

explorer\international[default\_codepage]

Queries value: HKCU\software\microsoft\internet explorer\international[autodetect]

Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color]

Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color visited]
Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color hover]
Queries value: HKCU\software\microsoft\internet explorer\settings[always use my colors]
Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font
sizel

Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font

face]

Queries value: HKCU\software\microsoft\internet explorer\settings[disable visited

hyperlinks]

Queries value: HKCU\software\microsoft\internet explorer\settings[use anchor hover

color1

Queries value: HKCU\software\microsoft\internet explorer\settings[miscflags]
Queries value: HKCU\software\microsoft\windows\currentversion\policies[allow

programmatic cut\_copy\_paste]

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

manager[pendingfilerenameoperations2]

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

manager[pendingfilerenameoperations]

Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefontsize]

Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefontsizeprivate] Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iepropfontname]

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefixedfontname]

Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage]

Queries value: HKLM\software\microsoft\internet explorer\version vector[vml]
Queries value: HKLM\software\microsoft\internet explorer\version vector[ie]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_zone\_elevation[71985e8a4de40ddc1151fafb929b5614.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation[\*]

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

settings\zones\0[2700]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[2700] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_xssfilter[71985e8a4de40ddc1151fafb929b5614.exe] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_xssfilter[\*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones[securitysafe] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nofileurl] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2106] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[2106] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]  $\label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet$ Oueries value: settings[cointernetcombineiuricachesize] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_subdownload\_lockdown[71985e8a4de40ddc1151fafb929b5614.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_subdownload\_lockdown[\*] HKCR\.css[content type] Oueries value: HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_behaviors[71985e8a4de40ddc1151fafb929b5614.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_behaviors[\*] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\0[2000] Queries value: HKLM\software\microsoft\internet explorer\default behaviors[discovery] HKCR\clsid\{3050f4cf-98b5-11cf-bb82-Oueries value: 00aa00bdce0b}\inprocserver32[inprocserver32]  $HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\tinprocserver32[]$ Queries value: Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid] HKCR\clsid\{3050f4cf-98b5-11cf-bb82-Oueries value: 00aa00bdce0b}\inprocserver32[threadingmodel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\0[1400] HKCR\.js[content type] Queries value: HKLM\software\microsoft\internet Queries value:  $explorer \verb|\main| feature control| feature_feeds [71985e8a4de40ddc1151fafb929b5614.exe]|$ HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_feeds[\*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonintranet] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[warnonintranet] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect] HKCR\clsid\{50d5107a-d278-4871-8989-Queries value: f4ceaaf59cfc}\inprocserver32[inprocserver32] HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[] Oueries value: Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid] HKCR\clsid\{50d5107a-d278-4871-8989-Queries value: f4ceaaf59cfc}\inprocserver32[threadingmodel1 Queries value: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable] Oueries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[inprocserver32] HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[] Queries value: Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid] HKCR\clsid\{3ce74de4-53d3-4d74-8b83-Oueries value: 431b3828ba53}\inprocserver32[threadingmodel] HKCR\clsid\{a4b544a1-438d-4b41-9325-Oueries value: 869523e2d6c7}\inprocserver32[inprocserver32] HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[] Oueries value: Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid] HKCR\clsid\{a4b544a1-438d-4b41-9325-Queries value: 869523e2d6c7}\inprocserver32[threadingmodel]

HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-Oueries value: 77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description] HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-Oueries value: 77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description] Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\selections.} \mbox{\tt url}$ Oueries value:

history[daystokeep]

HKCR\clsid\{f414c260-6ac0-11cf-b6d1-Oueries value:

00aa00bbbb58}\inprocserver32[inprocserver32]

 $HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\tinprocserver32[]$ Oueries value:

Queries value:  $HKCR \land \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} [appid]$ 

HKCR\clsid\{f414c260-6ac0-11cf-b6d1-Oueries value:

00aa00bbbb58}\inprocserver32[threadingmodel]

```
Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1201]
 Oueries value:
                           HKLM\system\currentcontrolset\control\nls\locale[00000409]
                           HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
 Oueries value:
                           HKLM\software\microsoft\ole[defaultaccesspermission]
 Queries value:
                           HKLM \setminus system \setminus current control \setminus lsa[everyone includes an onymous]
 Oueries value:
                           HKCR\.jpg[content type]
 Oueries value:
                           HKCR\.png[content type]
                           HKCR\clsid\{30c3b080-30fb-11d0-b724-
 Oueries value:
00aa006c1a01}\inprocserver32[inprocserver32]
                           HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
 Oueries value:
 Queries value:
                           HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}[appid]
 Queries value:
                           HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
                           HKCR\clsid\{6a01fda0-30df-11d0-b724-
 Queries value:
00aa006c1a01}\inprocserver32[inprocserver32]
                           HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
 Oueries value:
 Queries value:
                           HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
 Oueries value:
                           HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
 Queries value:
                           HKCR\mime\database\content type\image/bmp\bits[0]
 Queries value:
                           HKCR\mime\database\content type\image/gif\bits[0]
                           HKCR\mime\database\content type\image/jpeg\bits[0]
 Oueries value:
 Queries value:
                           HKCR\mime\database\content type\image/pjpeg\bits[0]
 Queries value:
                           HKCR\mime\database\content type\image/png\bits[0]
 Oueries value:
                           HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt image} \mbox{\tt x-png} \mbox{\tt bits} \mbox{\tt [0]}
 Queries value:
                           HKCR\mime\database\content type\image/x-wmf\bits[0]
 Queries value:
                           HKCR\mime\database\content type\image/x-png[image filter clsid]
 Queries value:
                           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
 Queries value:
                           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
                           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
 Oueries value:
 Queries value:
                           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
                           HKCU\software\microsoft\internet explorer\recovery[autorecover]
 Oueries value:
 Queries value:
                           HKCU\software\microsoft\ftp[use web based ftp]
 Queries value:
                           HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
                           HKCU\software\microsoft\internet explorer\suggested sites[enabled]
 Queries value:
                           HKLM\software\microsoft\internet explorer\feed discovery[sound]
 Queries value:
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2700]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[2700]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[]
                           HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings\5.0\user agent[]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[compatible]
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
 Queries value:
settings\5.0\user agent[compatible]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[version]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet settings[user
agent ]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
                           HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[71985e8a4de40ddc1151fafb929b5614.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[71985e8a4de40ddc1151fafb929b5614.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
 Queries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
 Oueries value:
                           HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
                           HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}[appid]
 Oueries value:
 Queries value:
                           HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\zones\3[1a10]
 Oueries value:
                           HKCU\software\microsoft\internet explorer\main[autosearch]
 Oueries value:
                           HKCU\software\microsoft\internet explorer\main[friendly http errors]
 Queries value:
                           HKLM\software\microsoft\internet explorer[version]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion[productname]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion[productname]
```

```
Queries value:
                                     HKLM\system\currentcontrolset\control\windows[csdversion]
                                     \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
  Oueries value:
settings\zones\3[currentlevel]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [allow file clsid junctions]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[progid]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[application]
  Queries value:
                                    HKCR\.htm[]
  Oueries value:
                                     HKCR\htmlfile\shellex\iconhandler[]
  Oueries value:
                                     HKCR\htmlfile[docobject]
  Queries value:
                                     HKCR\.htm[perceivedtype]
  Queries value:
                                     HKCR\systemfileassociations\text[docobject]
                                     HKCR\htmlfile[browseinplace]
  Oueries value:
  Queries value:
                                     HKCR\systemfileassociations\text[browseinplace]
  Oueries value:
                                     HKCR\htmlfile\clsid[]
  Oueries value:
                                     HKCR\htmlfile[isshortcut]
  Queries value:
                                     HKCR\systemfileassociations\text[isshortcut]
  Queries value:
                                     HKCR\htmlfile[alwaysshowext]
  Oueries value:
                                     HKCR\systemfileassociations\text[alwaysshowext]
  Queries value:
                                     HKCR\htmlfile[nevershowext]
  Queries value:
                                     HKCR\systemfileassociations\text[nevershowext]
  Oueries value:
                                     HKCU\appevents\schemes\apps\explorer\navigating\.current[]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:
                                     HKCU\control panel\desktop[lamebuttontext]
  Queries value:
                                     HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Queries value:
                                     HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[appid]
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[threadingmodel]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Oueries value:
                                     Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1258]
                                     HKLM\system\currentcontrolset\control\nls\codepage[874]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[932]
  Oueries value:
                                     HKLM \setminus system \setminus current control \setminus nls \setminus codepage \cite{Management} \cite{Managemen
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[949]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1361]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobject]
  Queries value:
  Oueries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[browseinplace]
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}\[isshortcut\]
  Queries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}[alwaysshowext]
  Oueries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[nevershowext]
  Oueries value:
                                     Oueries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-
  Queries value:
444553540000}\inprocserver32[loadwithoutcom]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
                                    HKCU\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x4011
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x4011
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-
  Oueries value:
444553540000}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
  Queries value:
  Queries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[threadingmodel]
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix]
```

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ 

Queries value:

```
settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions]
   Queries value:
                                                 HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
                                                 HKCR\.url\persistenthandler[]
   Oueries value:
   Queries value:
                                                 HKLM\software\microsoft\windows search[currentversion]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum[\{20d04fe0-3aea-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-10
08002b30309d}]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
   Queries value:
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[state]
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[userpreference]
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[centralprofile]
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[profileloadtimelow]
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[profileloadtimehigh]
   Queries value:
                                                 HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
   Oueries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\ windows \ system 32 \ shell 32.dll, -9216]
                                                 HKLM\software\microsoft\internet explorer\main[maxrenderline]
   Oueries value:
   Sets/Creates value:
                                                 HKCU\software\appdatalow\software\smartbar[globaluserid]
   Sets/Creates value:
                                                 HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
                                                 HKCU \setminus software \setminus conduit \setminus distribution engine \setminus 1 \setminus offerhistory \setminus 755131[offerid]
   Sets/Creates value:
   Sets/Creates value:
                                                 HKCU \setminus software \setminus conduit \setminus distribution engine \setminus 1 \setminus offerhistory \setminus 755131[offerurl]
   Sets/Creates value:
                                                 HKCU \setminus software \setminus conduit \setminus distribution engine \setminus 1 \setminus offerhistory \setminus 755131 [homapage]
   Sets/Creates value:
HKCU \setminus software \setminus conduit \setminus distribution engine \setminus 1 \setminus offerhistory \setminus 755131 [defaults earch]
   Sets/Creates value:
Sets/Creates value:
                                                 HKCU \setminus software \setminus conduit \setminus distribution engine \setminus 1 \setminus offerhistory \setminus 755131[ruleid]
   Sets/Creates value:
HKCU \setminus software \setminus conduit \setminus distribution engine \setminus 1 \setminus offerhistory \setminus 755131 [root offerid]
                                                 \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Sets/Creates value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
   Sets/Creates value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Sets/Creates value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit]
   Sets/Creates value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions]
   Sets/Creates value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair]
   Value changes:
                                                 HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ \{f90255c2-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7
806d6172696f}[baseclass]
   Value changes:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Value changes:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
   Value changes:
                                                 \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+shell
folders[historv]
   Value changes:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
   Value changes:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
   Value changes:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
   Value changes:
                                                 \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\connections[savedlegacysettings]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Value changes:
settings\zonemap[proxybypass]
   Value changes:
                                                 \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\zonemap[intranetname]
   Value changes:
                                                 HKCU\software\microsoft\windows\currentversion\internet
```

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

Value changes:

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

folders[local appdata]

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

 $\tt settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012016042820160429[cachepath]|$ 

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

folders[favorites]

Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]

Value changes: HKLM\system\currentcontrolset\control\session

manager[pendingfilerenameoperations]