Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 26, Task ID: 102

Task ID: 102 Risk Level: 7

Date Processed: 2016-04-28 12:49:11 (UTC)

Processing Time: 61.08 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe"

Sample ID: 26 Type: basic Owner: admin

Label: bdc27c485a35c61c7bf0bfedbf9b0b3f

Date Added: 2016-04-28 12:44:52 (UTC)

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

MD5: bdc27c485a35c61c7bf0bfedbf9b0b3f

SHA256: f89295cb1a70b1278e66a56acc10ee088a2ad2022664023d870c4698d0b4c7a1

Description: None

Pattern Matching Results

3 Long sleep detected

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

Static Events

YARA rule hit:	0LE2
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\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
["c:\windows\temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe"]
                                        C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe { "json_send_time" : "28/4/2016 14:49:54:686" , "product_id_version" : "" , "product_type" : "" , "product_id" : "" , "offer_id" : "77315" , "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": "000000000", "dm_version": "1.3.7.9_NoStatic.130521.01",
"bundle_id": "48dd2e32-2172-4f35-aac6-4a328190391d", "machine_user_id": "{6C411187-B302-4113-
B992-56B56F0A7EFC}" , "send_attempt" : "0" , "channel_id" : "" , "installation_session_id" :
"778F2147-88DC-4ED8-A85E-12949F8245E9" , "publisher_internal_id" : "" , "installation_session_id" : "778F2147-88DC-4ED8-A85E-12949F8245E9" , "publisher_internal_id" : "1" , "publisher_id" : "Brothersoft" , "order" : "1.0" , "phase" : "Init" , "Is_Test" : "0" }]
  Creates process:
                                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe { "user_ie_security_level" : "Unknown-0"
"json_send_time" : "28/4/2016 14:51:2:427" , "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/77256/?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": "77315", "general_status_code": "6", "duration_details": "InitPluginsDir:0
initializeParams:430 load BITool:31 send BI Init:60 load DownloadACC:70 retrieveUISource:10
unpack_webappfolder:0 unpack_icon:0 RetrieveMainOfferKey:0 unpack_OpenCandyDll:581
load_webapphost:0 unpack_ProxyInstaller:30 navigate_loadingUI:1241 navigateAsync_constMainOffer:0
BuildUserProfile:40 retrieve cid:10 callService1:62854 parse_ResponseXml:2184
init_external_offer:0 DiscoverUserAgent:210 " , "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": "00000000", "dm_version":
"1.3.7.9_NoStatic.130521.01" , "bundle_id" : "48dd2e32-2172-4f35-aac6-4a328190391d"
"machine_user_id" : "{6C411187-B302-4113-B992-56B56F0A7EFC}" , "send_attempt" : "0"
"channel_id" : "" , "installation_session_id" : "778F2147-88DC-4ED8-A85E-12949F8245E9"
```

```
"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\nse3.tmp\BI.exe

Named Object Events

```
Creates mutex:
                          \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003
                         \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-
 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
                         \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-
 Creates mutex:
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:
                         \BaseNamedObjects\ActiveSetupMutexId
 Creates mutex:
 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!
 Creates mutex:
                         \BaseNamedObjects\WininetConnectionMutex
 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.IDH
                          \BaseNamedObjects\userenv: User Profile setup event
 Creates event:
                          \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
 Creates semaphore:
 Creates semaphore:
                         \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
                          \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
 Creates semaphore:
                         \BaseNamedObjects\OleDfRoot000024B99
```

File Cyctem Fyente

Creates semaphore:

File System Events		
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsa2.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp</pre>	
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\nse3.tmp\System.dll</pre>	
Creates:	<pre>C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\System.dll</pre>	
Creates:	<pre>C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nse3.tmp\webapphost.dll		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\BI.exe</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nse3.tmp\DM_loader.gif		
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nse3.tmp\DownloadACC.exe		
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\icon.png</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nse3.tmp\OCSetupHlp.dll		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsv4.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nst5.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp</pre>	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn6.tmp	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\inetc.dll	
Creates:	<pre>C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\webapphost.dll</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\a.txt</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nse3.tmp\ProxyInstaller.exe		
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\~DF4B9C.tmp	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\inetc.dll</pre>	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\offer.xml	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temporary Internet	
Files\Content.IE5\QXMNQBKF\navcancl[1]		
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn6.tmp\inetc.dll	
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
 Creates:
Files\Content.IE5\UH4D6D6X\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\bullet[1]
                         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
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Creates:
Files\Content.IE5\CXCXW1MR\dnserrordiagoff_web0C[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
 Creates:
Files\Content.IE5\UH4D6D6X\down[1]
                         {\tt 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\down[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\UH4D6D6X\dnserrordiagoff web0C[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\QXMNQBKF\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\xml.dll
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\xml.dll
 Creates:
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\nsArray.dl1
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\nsArray.dll
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\OXMNOBKF\down[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsy7.tmp
 Creates:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nss8.tmp}
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm9.tmp
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\inetc.dll
 Creates:
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\History\History.IE5\MSHist012016042820160429
 Creates:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\a.txt
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm9.tmp\netc.dll
 Creates:
                         C:\WINDOWS\Prefetch\BDC27C485A35C61C7BF0BFEDBF9B0-17324D5A.pf
 Opens:
 Opens:
                         C:\Documents and Settings\Admin
 Opens:
                         C:\WINDOWS\system32\imm32.dll
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\svstem32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\WindowsShell.Config
```

```
C:\WINDOWS\Temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
  Opens:
  Opens:
                                           C:\windows\temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe.124.Manifest
                                           C:\WINDOWS\system32\comctl32.dll
  Opens:
  Opens:
                                           C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
  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:
  Opens:
                                           C:\Documents and Settings
                                           C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp
  Opens:
  Opens:
                                           C:\WINDOWS\Temp\42f86ce3-3213-45b1-8684-b119ee2cb467
                                           C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:
  Opens:
                                           C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp
                                           C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\System.dll
  Opens:
  Opens:
                                           C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\webapphost.dll
  Opens:
                                           C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\webapphost.dll.2.Manifest
                                           C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\webapphost.dll.2.Config
  Opens:
  Opens:
                                           C:\WINDOWS\system32\winspool.drv
                                           C:\WINDOWS\system32\oledlg.dll
  Opens:
  Opens:
                                           C:\WINDOWS\system32\crypt32.dll
  Opens:
                                           C:\WINDOWS\system32\msasn1.dll
  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
                                           C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:
  Opens:
                                           C:\WINDOWS\system32\WININET.dll.123.Manifest
  Opens:
                                           C:\WINDOWS\system32\WININET.dll.123.Config
                                           \label{locals-locals-locals-locals-locals-locals-locals-local} C: \DOCUME \sim 1 \land Admin \land LOCALS \sim 1 \land Temp \land s = 1 \land Locals \land Lo
  Opens:
  Opens:
                                           {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nse3.tmp\BI.exe}
  Opens:
                                           C:\WINDOWS\system32\apphelp.dll
  Opens:
                                           C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:
                                           C:\WINDOWS\AppPatch\systest.sdb
  Opens:
                                           C:\Documents and Settings\Admin\Local Settings
                                           C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe.Manifest
  Opens:
  Opens:
                                           C:\WINDOWS\Prefetch\BI.EXE-35A91DD2.pf
  Opens:
                                           C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe.124.Manifest
  Opens:
                                           {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsv4.tmp}
  Opens:
                                           C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp
  Opens:
                                           C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\inetc.dll
                                           C:\WINDOWS\Fonts\sserife.fon
  Opens:
  Opens:
                                           C:\WINDOWS\system32\MSCTFIME.IME
  Opens:
                                           C:\WINDOWS\system32\MSIMTF.dll
                                           C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
  Opens:
  Opens:
                                           C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
                                           C:\Documents and Settings\Admin\Local Settings\History
  Opens:
  Opens:
                                           C:\Documents and Settings\Admin\Local Settings\History\History.IE5
  Opens:
                                           C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
                                           C:\Documents and Settings\Admin\Cookies
  Opens:
  Opens:
                                           C:\Documents and Settings\Admin\Cookies\index.dat
                                           C:\Documents and Settings\Admin\Local
  Opens:
Settings\History\History.IE5\index.dat
                                           C:\WINDOWS\system32\ws2 32.dll
  Opens:
                                           C:\WINDOWS\system32\ws2help.dll
  Opens:
  Opens:
                                           C:\WINDOWS\system32\rasapi32.dll
  Opens:
                                           C:\WINDOWS\system32\rasman.dll
  Opens:
                                           C:\WINDOWS\system32\netapi32.dll
  Opens:
                                           C:\WINDOWS\system32\tapi32.dll
  Opens:
                                           C:\WINDOWS\system32\rtutils.dll
  Opens:
                                           C:\WINDOWS\system32\winmm.dll
  Opens:
                                           C:\WINDOWS\system32\TAPI32.dll.124.Manifest
  Opens:
                                           C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:
                                           C:\AUTOEXEC.BAT
  Opens:
                                           C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
                                           C:\WINDOWS\system32\ras
  Opens:
                                           C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Network\Connections\Pbk\
                                           C:\WINDOWS\system32\sensapi.dll
  Opens:
  Opens:
                                           C:\WINDOWS\system32\mswsock.dll
  Opens:
                                           C:\WINDOWS\system32\rasadhlp.dll
                                           C:\WINDOWS\system32\dnsapi.dll
  Opens:
  Opens:
                                           C:\WINDOWS\system32\iphlpapi.dll
  Opens:
                                           C:\WINDOWS\system32\drivers\etc\hosts
  Opens:
                                           C:\WINDOWS\system32\rsaenh.dll
  Opens:
                                           C:\WINDOWS\system32\asycfilt.dll
  Opens:
                                           C:\WINDOWS\system32\msv1_0.dll
  Opens:
                                           C:\WINDOWS\system32\clbcatq.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
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nse3.tmp\linetc.dll}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\icon.png
 Opens:
                         C:\WINDOWS\system32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[2]
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\a.txt
 Opens:
 Opens:
                         C:\WINDOWS\system32\psapi.dll
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn6.tmp\
                         C:\WINDOWS\system32\mlang.dll
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\OXMNOBKF\navcancl[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\navcancl[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
 Opens:
                         C:\WINDOWS\system32\iepeers.dll
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Manifest
                         C:\WINDOWS\system32\iepeers.dll.123.Config
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                         C:\WINDOWS\system32\jscript.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
 Opens:
                         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]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[1]
                         C:\WINDOWS\system32\imgutil.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
                         C:\WINDOWS\system32\pngfilt.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\info_48[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[2]
                         C:\WINDOWS\Fonts\SEGOEUI.TTF
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR
 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\QXMNQBKF\httpErrorPagesScripts[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\down[1]
 Opens:
                         C:\WINDOWS\Fonts\wingding.ttf
                         C:\WINDOWS\system32\en-US\mshtml.dll.mui
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\CXCXW1MR\dnserrordiagoff_web0C[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_web0C[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\background_gradient[2]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\info_48[2]
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\xml.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\offer.xml
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\nsArray.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[2]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[2]
 Opens:
                         C:\WINDOWS\system32\config
 Opens:
                         C:\WINDOWS\system32\drivers
 Opens:
 Opens:
                         C:\WINDOWS\system32\drivers\etc
 Opens:
                         C:\WINDOWS\Temp
                         C:\WINDOWS\WinSxS
 Opens:
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
 Opens:
                         C:\WINDOWS\system32\locale.nls
 Opens:
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dll
 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
                         C:\WINDOWS\system32\ctype.nls
 Opens:
 Opens:
                         C:\WINDOWS\system32\sortkey.nls
 Opens:
                         C:\WINDOWS\system32\wininet.dll
                         C:\WINDOWS\system32\normaliz.dll
 Opens:
 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
                         C:\WINDOWS\Temp\42f86ce3-3213-45b1-8684-b119ee2cb467\969_inetc.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
                         C:\WINDOWS\Fonts\arialbd.ttf
 Opens:
 Opens:
                         C:\WINDOWS\Fonts\verdana.ttf
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsy7.tmp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014033120140407\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\inetc.dll
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014041220140413\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings \verb|\History\History.IE5\MSHist012016042820160429|
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\a.txt
 Opens:
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm9.tmp\
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsa2.tmp
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\System.dll
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\webapphost.dll
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\BI.exe
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\DM_loader.gif
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\DownloadACC.exe
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\icon.png
```

```
C:\Documents and Settings\Admin\Local Settings\Temp\nst5.tmp
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\inetc.dll
 Writes to:
 Writes to:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\OCSetupHlp.dll
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\ProxyInstaller.exe
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\inetc.dll
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\navcancl[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\navcancl[11
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\info_48[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\bullet[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
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
 Writes to:
Files\Content.IE5\UH4D6D6X\info_48[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\bullet[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         {\tt 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
 Writes to:
Files\Content.IE5\CXCXW1MR\dnserrordiagoff_web0C[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\down[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
Files\Content.IE5\QXMNQBKF\down[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_web0C[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
Files\Content.IE5\QXMNQBKF\bullet[2]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\offer.xml
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\xml.dll
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\nsArray.dll
 Writes to:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Writes to:
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
                         {\tt 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
Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temp\nss8.tmp
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\inetc.dll
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
 Reads from:
                         C:\WINDOWS\Temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsa2.tmp
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\BI.exe
                          C:\Documents and Settings\Admin\Local Settings\Temp\nst5.tmp
 Reads from:
 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\nse3.tmp\offer.xml
```

```
Reads from:
                          C:\WINDOWS\Prefetch\BI.EXE-35A91DD2.pf
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm
                          C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nss8.tmp
 Reads from:
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsv4.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp
 Deletes:
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[2]
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\a.txt
 Deletes:
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.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
 Deletes:
Files\Content.IE5\UH4D6D6X\navcancl[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
 Deletes:
                          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]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\UH4D6D6X\background_gradient[1]
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Deletes:
Files\Content.IE5\UH4D6D6X\info_48[1]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Deletes:
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[1]
 Deletes:
                          {\tt 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
 Deletes:
Files\Content.IE5\UH4D6D6X\bullet[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\info 48[1]
 Deletes:
                          {\tt 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\dnserrordiagoff_webOC[1]
                          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\UH4D6D6X\down[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\CXCXW1MR\dnserrordiagoff_web0C[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_web0C[1]
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Deletes:
Files\Content.IE5\QXMNQBKF\background_gradient[2]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\info_48[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\bullet[2]
 Deletes:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[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\Temp\nsy7.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
 Deletes:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\a.txt
 Deletes:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsm9.tmp\inetc.dll}
```

Network Events

ude.conduit-data.com DNS query:

DNS auerv: 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: 127.0.0.1:1053 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:

806d6172696f}\

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

Creates key: HKCU\software

Creates key: HKCU\software\appdatalow

Creates key: HKCU\software\appdatalow\software

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \ \ \mbox{\tt settings} \ \ \mbox{\tt microsoft\windows\currentversion\color=lem:} \ \mb$ Creates key: Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell} folders}$ Creates kev:

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

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

awareness

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

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

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

 $HKCU \ software \ \verb|\conduit\| distribution engine \ \verb|\conduit\| ferhistory \ \ ferhistory \ \$ Creates kev:

Creates key: HKCU\software\conduit

Creates key: $\label{lem:hkcu} \verb+KCU\+ software\+ conduit\+ distribution engine$ Creates key: HKCU\software\conduit\distributionengine\1

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

settings\5.0\cache\extensible cache\mshist012016042820160429

HKCU\software\microsoft\internet explorer\main\windowssearch Creates key: Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe

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

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

options\gdi32.dll

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

options\user32.dll

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

Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

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

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

Opens key:

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

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

options\shlwapi.dll

Opens key:

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

options\shell32.dll

Opens kev:

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

options\comctl32.dll

Opens key:

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

options\ole32.dll

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

options\version.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKLM\

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

Opens key: HKLM\system\setup

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

Opens key:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{\current} version \label{lem:hklm} idebyside \label{lem:hklm} \label{lkm} \label{lkm}$

Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced$ Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack

HKLM\software\microsoft\ole Opens key:

Opens key: HKCR\interface

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

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

options\msctf.dll

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus bdc27c485a35c61c7bf0bfedbf9b0b3f.exe$

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

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

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

options\shfolder.dll

HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt$

Opens key:

a2d8-08002b30309d}

Opens key: HKCU\software\classes\

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

08002b30309d}\inprocserver32

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32 Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\setupapi.dll

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

Opens key: HKLM\system\wpa\pnp

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

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

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

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

Opens key: HKLM\software\microsoft\rpc

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

options\bdc27c485a35c61c7bf0bfedbf9b0b3f.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:

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}

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

409d6c4515e9}

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

Opens kev: HKCU\software\microsoft\windows\currentversion\explorer Opens key: HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: HKCU\software\microsoft\windows\currentversion\policies\system Opens key: HKCU\software\classes\directory\shellex\iconhandler Opens key: HKCR\directory\shellex\iconhandler HKCU\software\classes\directory\clsid Opens key: Opens key: HKCR\directorv\clsid Opens key: HKCU\software\classes\folder Opens key: HKCR\folder HKCU\software\classes\folder\clsid Opens key:

Opens key: HKCR\folder\clsid

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

options\system.dll

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

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

options\comdlg32.dll

Opens key: options\winspool.drv HKLM\software\microsoft\windows nt\currentversion\image file execution

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

options\oledlg.dll

Opens key: HKCU\software\classes\clsid

Opens key: HKCR\clsid

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens kev:

options\oleaut32.dll

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

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

options\msasn1.dll

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

options\crypt32.dll

Opens key: HKLM\system\currentcontrolset\services\crypt32\performance $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hklm}\software\mbox{$\mbox{microsoft}\windows}$ nt\currentversion\mbox{$\mbox{msasn1}$} \mbox{$\mbox{$\mbox{exp}$}$} \mbox{$\mbox{\m Opens key:

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

options\normaliz.dll

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

options\iertutil.dll

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

options\urlmon.dll

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

Opens key: HKCR\protocols\name-space handler

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

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

settings

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

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

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

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

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

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

settings\zonemap\domains\

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

settings\zonemap\ranges\

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

settings\zonemap\ranges\

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

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\bi.exe

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

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

Opens key:

be2efd2c1a33}

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

Opens key:

Opens key:

Opens key:

Opens key:

Opens key:

Opens key:

 $\label{local-policies} HKLM \software \policies \microsoft \windows \safer \code identifiers \oldsymbol{local-policies} \label{local-policies} WLLM \software \policies \microsoft \windows \safer \code identifiers \oldsymbol{local-policies} \label{local-policies} \parbox{\sim} \parbox{\sim}$

Opens key:

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

KLM\ softw

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} White \label{lem:hklm} \label{lem:hklm} White \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} HKLM \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} White \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} White \label{lem:hkklm} \label{lem:hkklm} White \label{lem:hkklm} \label{lem$

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

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} with the local property of the local property of$

Opens key:

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

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths

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

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

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes

Opens key:

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

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

Opens key:

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

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths

Opens key:

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

Opens kev:

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

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 kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes

Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus urlzones$

Opens key:

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

Opens key:

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

Opens key:

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\bi.exe

Opens key: HKLM\software\microsoft\ctf\compatibility\bi.exe

 $Opens \ key: \\ HKLM \ software \ microsoft \ windows \ nt \ current version \ image \ file \ execution options \ bi.exe \ rpcthread pool throttle$

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

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 key: HKCU\software\microsoft\ctf

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

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

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

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

 $Opens\;key: \\ \qquad \qquad \text{HKLM} \\ \text{software} \\ \text{microsoft} \\ \text{windows} \\ \text{currentversion} \\ \text{internet}$

settings\5.0\cache\content

 $Opens\ key: \\ \hspace{1.5cm} \text{HKCU} \\ software \\ \text{microsoft} \\ \text{windows} \\ \text{current} \\ \text{version} \\ \text{internet}$

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

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

settings\5.0\cache\history

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

settings\5.0\cache\history

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

Opens key: $\label{thm:consoftware} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\linear}} \mbox{\colored}$

settings\5.0\cache\extensible cache\feedplat

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

settings\5.0\cache\extensible cache\iecompat

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

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\cur

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

settings\5.0\cache\extensible cache\mshist012014041220140413

 $Opens~key: \\ \hspace*{0.2cm} \textit{HKCU} software \verb|microsoft| windows \verb|currentversion| internet| \\$

settings\5.0\cache\extensible cache\privacie:

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer| \verb|main| feature control| retry_header on ly post_on connection reset| \\$

Opens key: HKLM\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\retry_headeronly post_on connection reset|\\$

explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954

Opens key: HKLM\software\microsoft\internet

settings\5.0\cache

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

settings\5.0\cache

Opens key: HKCU\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_fix_chunked_proxy_script_download_kb843289$

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

Opens key: HKLM\software\microsoft\internet
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

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_allow_long_international_filenames| \\$

Opens key: HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_allow_long_international_filenames
                    HKCU\software\microsoft\internet
 Opens kev:
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
 Opens key:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                    HKCU\software\microsoft\internet
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 key:
                    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
                    HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
                    HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\ws2_32.dll
 Opens key:
                     HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens kev:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000003
 Opens key:
Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens key:
Opens key:
Opens key:
                    \label{thm:local_hammon} \mbox{HKCU\software\mbox{\sc urrentversion\internet settings\wpad}} \  \,
 Opens kev:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                    HKLM\software\microsoft\internet
 Opens kev:
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
 Opens key:
                    HKCU\software\microsoft\windows\currentversion\internet settings\http
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
```

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

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

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

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

options\netapi32.dll

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

options\rasman.dll

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

options\rtutils.dll

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

options\winmm.dll

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

Opens key:

options\tapi32.dll

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

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

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

options\rasapi32.dll

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

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

options\userenv.dll

Opens key:

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: HKLM\system\currentcontrolset\control\session manager\environment

HKU\ Opens key:

Opens key:

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

Opens key: HKCU\volatile environment

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

options\sensapi.dll

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

options\mswsock.dll

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

Opens kev:

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

options\dnsapi.dll

Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

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\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}

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

cryptographic provider

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

 ${\it HKLM \ } system \ `current control \ 'security providers$ Opens key: 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\windows nt\currentversion\image file execution

options\asycfilt.dll

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

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

472f-a0ff-e1416b8b2e3a}

HKLM\software\microsoft\com3 Opens kev:

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

options\comres.dll

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

options\clbcatq.dll

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

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

Opens key: $HKLM\software\microsoft\net\ framework\ setup\ndp\v2.0.50727$

Opens key: HKLM\software\classes

Opens key: $HKLM\software\microsoft\net framework setup\ndp\v3.0$ Opens key: HKLM\software\microsoft\net framework setup\ndp\v3.5

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

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

00c04fd705a2}\treatas

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

00c04fd705a2}\inprocserver32

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

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

Opens key: HKCU\software\conduit\distributionengine\1\offerhistory Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserverx86

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

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 kev:

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

00c04fd705a2}\localserver

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

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

options\rsaenh.dll

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

0000c05bae0b}\typelib

 $HKCR\interface \\ \{eab22ac1-30c1-11cf-a7eb-0000c05bae0b\} \\ typelib$ Opens key: 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-

00000000046}\proxystubclsid32

Opens key: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32

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

00c04f79abd1}\proxystubclsid32

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

HKCU\software\microsoft\internet Opens key:

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

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

Opens kev: HKCU\software\policies\microsoft\internet explorer\main

Opens key:

a2ea-08002b30309d}

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

08002b30309d}\inprocserver32

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

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

08002b30309d}\localserver32

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

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

08002b30309d}\inprochandler32

Opens key: $HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\tinprochandler 32$

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

08002b30309d}\inprochandlerx86

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

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

```
HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_iedde_register_protocol
                         HKLM\software\policies\microsoft\internet explorer\browseremulation
 Opens kev:
                         HKCU\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
 Opens kev:
                         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\*\
                         HKCR\protocols\name-space handler\*
 Opens key:
 Opens key:
                         HKCU\software\classes\protocols\handler\res
 Opens key:
                         HKCR\protocols\handler\res
                         HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
 Opens key:
                         HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
                         HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\treatas
 Opens key:
                         HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas
                         HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
 Opens key:
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
                         HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
 Opens key:
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:
                         \label{lem:hkcr} $HKCR\clsid{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\ender 32$
 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 \verb|\clsid|{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\\ \\ local server
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msls31.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mshtml.dll
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKCU\software\microsoft\internet
 Opens key:
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
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                         HKLM\software\microsoft\internet
 Opens kev:
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
 Opens kev:
                         HKCU\software\microsoft\internet
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 kev:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
 Opens kev:
                         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 kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key:
                          HKCU\software\microsoft\internet
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 key:
                          HKCU\software\microsoft\internet explorer\domstorage
 Opens key:
                          HKLM\software\microsoft\internet explorer\domstorage
 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:
                          HKLM\software\microsoft\internet explorer\safety\privacie
 Opens kev:
 Opens key:
                          HKLM\software\policies\microsoft\cryptography
 Opens key:
                          HKLM\software\microsoft\internet explorer\mediatypeclass
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\policies\ratings
                         HKLM\software\microsoft\cryptography
 Opens key:
 Opens key:
                          HKLM\software\microsoft\cryptography\offload
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
 Opens key:
                          HKLM\system\currentcontrolset\services\winsock\parameters
                          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens key:
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\zonemap\protocoldefaults\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\domains\
                          HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
                         \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
 Opens key:
settings\zonemap\domains\msn.com
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com\related
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\wshtcpip.dll
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                         HKLM\software\microsoft\internet
explorer \verb|\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
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
```

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

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

Opens key:

```
settings\zones\0
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones\1
  Opens key:
                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:
                                       \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\2
                                       HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\2
  Opens key:
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:
                                       \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\zones\3
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\4
  Opens key:
                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:
                                       HKCU\software\microsoft\internet
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\
  Opens key:
                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
  Opens key:
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\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
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\3
  Opens key:
                                       \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\3
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
                                       \label{lem:hklmsoftware policies microsoft windows \current version \cite{thmsoftware} in the lemma of the 
  Opens key:
settings\lockdown_zones\4
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                      HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
                                      HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
                                      HKCU\software\microsoft\internet explorer
  Opens key:
                                       HKLM\software\microsoft\internet explorer
                                      HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_restrict_res_to_lmz
                                      HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature restrict res to lmz
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_load_shdoclc_resources
                                      HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_load_shdoclc_resources
                                       HKCU\software\classes\.htm
  Opens kev:
  Opens key:
                                      HKCR\.htm
  Opens key:
                                      HKCU\software\classes\protocols\filter\text/html
  Opens key:
                                       HKCR\protocols\filter\text/html
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                                      HKLM\software\microsoft\internet
  Opens kev:
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
```

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

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

00aa00686f13}\treatas

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

00aa00686f13}\inprocserver32

Opens key: $\label{lem:hkcr} \mbox{HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\} \mbox{inprocserver32}$

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

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

00aa00686f13}\inprochandlerx86

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

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

00aa00686f13}\localserver

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

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

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

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

detection

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

detection

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

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

Opens key: HKCR\protocols\handler\about

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

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

00aa00bdce0b}\treatas

Opens key: $\begin{tabular}{ll} HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-10ef-bb82-11ef-b$

00aa00bdce0b}\inprocserver32

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32

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

 $Opens~key: \\ HKLM\software\microsoft\windows\currentversion\sinternet~settings\cones\cite{Constraints} \\$

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: 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

```
HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer
                                    HKCU\software\microsoft\internet explorer\international
  Opens key:
  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
                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus active desktop
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\policies
                                    HKCU\software\microsoft\internet explorer\pagesetup
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet explorer\menuext
                                    HKCU\software\microsoft\internet explorer\menuext\%s
  Opens key:
  Opens key:
                                    HKI M\system\currentcontrolset\control\nls\codepage
                                    HKCU\software\microsoft\internet explorer\international\scripts\3
  Opens key:
  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
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
                                   HKCU\software\microsoft\internet
  Opens key:
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
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
  Opens key:
                                    \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \sides \current} \end{tabular} \begin{tabular}{ll} All \sides \mbox{$\mbox{$microsoft$} \sides \sides \current} \end{tabular} \begin{tabular}{ll} All \sides \mbox{$\mbox{$microsoft$} \sides \sides
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_shim_mshelp_combine
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
                                   HKCU\software\classes\.css
  Opens key:
  Opens key:
                                    HKCR\.css
  Opens key:
                                    HKCU\software\classes\protocols\filter\text/css
                                   HKCR\protocols\filter\text/css
  Opens key:
  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
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
                                    HKLM\software\microsoft\internet
  Opens kev:
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}
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                    Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\tinprocserver32
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
                                   HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens key:
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\tinprochandler32
```

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

00aa00bdce0b}\inprochandlerx86

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

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

00aa00bdce0b}\localserver

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

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\main\featurecontrol\feature_binary_caller_service_provider

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

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

Opens key: HKCU\software\classes\.js

Opens key: HKCR\.js

Opens key: HKCU\software\microsoft\internet

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

settings\zonemap\

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

settings\zonemap\

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

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

f4ceaaf59cfc}\treatas

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

f4ceaaf59cfc}\inprocserver32

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

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

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

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

f4ceaaf59cfc}\inprochandler32

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32 Opens key:

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

f4ceaaf59cfc}\inprochandlerx86

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86 Opens key:

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

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 key: HKLM\software\microsoft\ctf\tip

Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

c9633f71be64}\languageprofile

Opens key:

c9633f71be64}\languageprofile

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ Opens key:

c9633f71be64}\languageprofile\0x00000000

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ Opens kev: c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}

Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53} HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens key:

431b3828ba53}\treatas

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas Opens kev: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-

Opens key:

431b3828ba53}\inprocserver32 Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32

Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\inprocserverx86

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86 Opens key:

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 kev:
                                                                                                                                           HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
          Opens key:
                                                                                                                                           HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
  431b3828ba53}\inprochandlerx86
                                                                                                                                          HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86
          Opens key:
          Opens key:
                                                                                                                                           HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
 431b3828ba53}\localserver
                                                                                                                                           HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
          Opens key:
          Opens key:
                                                                                                                                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{a4b544a1-438d-4b41-9325-869523e2d6c7\}
          Opens key:
                                                                                                                                           HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
                                                                                                                                           HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
          Opens key:
 869523e2d6c7}\treatas
                                                                                                                                           HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
          Opens key:
                                                                                                                                           HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
          Opens key:
  869523e2d6c7}\inprocserver32
          Opens key:
                                                                                                                                           HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32
          Opens key:
                                                                                                                                           HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
 869523e2d6c7}\inprocserverx86
          Opens key:
                                                                                                                                           HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
          Opens kev:
                                                                                                                                          HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
  869523e2d6c7}\localserver32
          Opens key:
                                                                                                                                          HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
                                                                                                                                           Opens key:
 869523e2d6c7}\inprochandler32
          Opens key:
                                                                                                                                           HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
                                                                                                                                           HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
          Opens kev:
  869523e2d6c7}\inprochandlerx86
          Opens key:
                                                                                                                                          HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
                                                                                                                                          HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
          Opens key:
 869523e2d6c7}\localserver
          Opens key:
                                                                                                                                           HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
                                                                                                                                           HKLM\software\microsoft\ctf\tip\
          Opens key:
          Opens key:
                                                                                                                                           HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
 c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                                           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
          Opens key:
 77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                                           HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
          Opens key:
 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\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                                           HKLM \setminus software \setminus irrosoft \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-bd2f
          Opens key:
 Of816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                                           HKCU\software\microsoft\ctf\langbaraddin\
          Opens key:
          Opens key:
                                                                                                                                           HKLM\software\microsoft\ctf\langbaraddin\
          Opens key:
                                                                                                                                           HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
 c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
          Opens key:
                                                                                                                                           HKLM \setminus software \setminus icrosoft \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-4fcc
  77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                                                           HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
         Opens key:
 e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                                                           HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
          Opens key:
 00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
          Opens key:
                                                                                                                                           HKLM \setminus software \setminus microsoft \setminus tip \setminus \{f89e9e58 - bd2f - 4008 - 9ac2 - bd2f - 4008 - b
  Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                                                           HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
          Opens key
 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}
                                                                                                                                           HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
         Opens key:
  c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                                                                           HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
          Opens kev:
  77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                                                                           HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
          Opens kev:
  c9633f71be64\\ \\ category\\ \\ item\\ \\ c6debc0a-f2b2-4f17-930e-ca9faff4cd04\\ \\ \\
                                                                                                                                           HKLM \setminus software \setminus irrosoft \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-4fcc
          Opens key:
  77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
          Opens kev:
                                                                                                                                           HKCU\software\policies\microsoft\internet explorer\control panel
          Opens key:
                                                                                                                                           HKCU\software\microsoft\windows\currentversion\internet settings\url
history
         Opens kev:
                                                                                                                                          HKCU\software\microsoft\internet
  explorer\main\featurecontrol\feature_iedde_register_urlecho
          Opens key:
                                                                                                                                          HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_iedde_register_urlecho
          Opens key:
                                                                                                                                           HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
          Opens key:
                                                                                                                                           HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
          Opens key:
                                                                                                                                           HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
 00aa00bbbb58}\treatas
                                                                                                                                           HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\}\treatas
          Opens key:
                                                                                                                                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{f414c260-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac
          Opens kev:
 00aa00bbbb58}\inprocserver32
```

 $HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbb58\\\inprocserver32$ Opens key:

HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-Opens key:

00aa00bbbb58}\inprocserverx86

HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86 Opens key:

Opens kev: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\localserver32

Opens key: $HKCR \clsid \f414c260-6ac0-11cf-b6d1-00aa00bbbb58 \localserver 32$

HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-Opens key:

00aa00bbbb58}\inprochandler32

 $HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprochandler32$ Opens key:

Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprochandlerx86

Opens key: $HKCR \ clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbb58\} \ in prochandler x86$

HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-Opens key:

00aa00bbbb58}\localserver

HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver Opens key:

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

options\jscript.dll

Opens key: HKLM\software\microsoft\windows script\features

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547

Opens key: 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 HKLM\system\currentcontrolset\control\nls\language groups Opens kev: Opens key: HKCU\software\classes\appid\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe

Opens key: HKCR\appid\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_scripturl_mitigation Opens key: HKCU\software\classes\.jpg

Opens key: HKCR\.jpg

Opens key: HKCU\software\classes\protocols\filter\image/jpeg

Opens key: HKCR\protocols\filter\image/jpeg HKCU\software\classes\.png Opens key:

HKCR\.png Opens key:

Opens key: HKCU\software\classes\protocols\filter\image/png

HKCR\protocols\filter\image/png Opens key: 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

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{30c3b080-30fb-11d0-b724-00aa006c1a01\}$ Opens key:

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01} Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\treatas

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprocserver32

Opens key: $HKCR \c1sid \c3oc3b080-30fb-11d0-b724-00aa006c1a01 \c1oprocserver 32$

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprocserverx86

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86 Opens key:

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\localserver32

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprochandler32

Opens key: $HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\inprochandler32$

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprochandlerx86

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\localserver

Opens key: $\label{localserver} $HKCR\clsid{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver $$ $HKCR\clsid{30c3b080-30b0$ HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} Opens kev:

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

00aa006c1a01}\treatas

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

00aa006c1a01}\inprocserver32

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

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

00aa006c1a01}\inprocserverx86

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

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

00aa006c1a01}\localserver32

Opens key: $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32$

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

00aa006c1a01}\inprochandler32

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

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

00aa006c1a01}\inprochandlerx86

 $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\timerochandlerx86$ Opens key:

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

00aa006c1a01}\localserver

 $HKCR \clsid \end{6a01fda} -30df-11d0-b724-00aa006c1a01 \end{6a01fda} -local server$ Opens key:

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

HKCR\mime\database\content type Opens kev:

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

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

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

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: 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

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \simple \classes \mime \mime$ Opens key:

Opens key: $\label{lem:hkcr} \mbox{HKCR} $$ \mbox{HKCR} \rightarrow \mbox{HKCR} $$ is a parameter of the lambda of the l$

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

 $HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt image} \mbox{\tt x-png} \mbox{\tt bits}$ Opens key:

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

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

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \slimage \slimage \slimage \classes \mime \slimage \sl$ Opens key:

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

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

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

00a0c913f750}\treatas

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

00a0c913f750}\inprocserver32

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

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

00a0c913f750}\inprocserverx86

 $HKCR\clsid\\a3ccedf7-2de2-11d0-86f4-00a0c913f750\\\label{eq:hkcr} \\\label{eq:hkcr} \\\label{eq:hkcr}$ Opens key:

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

00a0c913f750}\localserver32

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

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

00a0c913f750}\inprochandler32

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

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

00a0c913f750}\inprochandlerx86

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

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

00a0c913f750}\localserver

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

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

options\pngfilt.dll

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

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:

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: HKLM\software\policies\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 HKLM\software\microsoft\internet explorer\feed discovery Opens key:

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_isolate_named_windows HKLM\software\microsoft\internet Opens kev: $\verb|explorer\main\featurecontrol\feature_isolate_named_windows|\\$ HKCU\software\classes\protocols\name-space handler\http\ Opens key: Opens key: HKCR\protocols\name-space handler\http Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent HKCU\software\microsoft\windows\currentversion\internet 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 HKCU\software\microsoft\windows\currentversion\internet Opens key: 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 HKCU\software\microsoft\internet Opens key: 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 HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_legacy_compression Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893f - fd2b31b3eefd\}$ Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd} Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\treatas Opens key: $HKCR\clsid\ensuremath{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treats$ Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\inprocserver32 Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32 HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-Opens kev: fd2b31b3eefd}\inprocserverx86 HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserverx86 Opens key: Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\localserver32 Opens key: $HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver32$ Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\inprochandler32 $HKCR\clsid\ensuremath{\clsi}$ Opens key: Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\inprochandlerx86 Opens key: Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\localserver HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_disable_navigation_sounds HKLM\software\microsoft\internet Opens kev: 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

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

options\xml.dll

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

options\nsarray.dll

Opens kev: HKLM\svstem\currentcontrolset\control\windows

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file exts \end{tabular}$

```
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
  Opens key:
  Opens key:
                                        HKCU\software\classes\htmlfile
                                        HKCR\htmlfile
  Opens kev:
  Opens key:
                                        HKCU\software\classes\htmlfile\curver
  Opens kev:
                                        HKCR\htmlfile\curver
  Opens key:
                                        HKCR\htmlfile\
                                        HKCU\software\classes\htmlfile\shellex\iconhandler
  Opens key:
  Opens key:
                                        HKCR\htmlfile\shellex\iconhandler
  Opens key:
                                        HKCU\software\classes\systemfileassociations\.htm
                                        HKCR\systemfileassociations\.htm
  Opens key:
  Opens key:
                                        HKCU\software\classes\systemfileassociations\text
  Opens key:
                                        HKCR\systemfileassociations\text
  Opens key:
                                        HKCU\software\classes\htmlfile\clsid
                                        HKCR\htmlfile\clsid
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}
  Opens key:
                                       HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented
categories\{00021490-0000-0000-c000-00000000046}
  Opens key:
                                        HKCU\appevents\schemes\apps\explorer\navigating\.current
  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:
                                        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}
                                        HKCU\software\classes\*
  Opens key:
  Opens key:
                                        HKCR\*
  Opens key:
                                        HKCU\software\classes\*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
                                        HKCR\*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
  Opens key:
  Opens key:
                                        HKCU\software\classes\htmlfile\shellex\{000214e6-0000-0000-c000-
00000000046}
                                        HKCR\htmlfile\shellex\{000214e6-0000-0000-c000-00000000046}
  Opens key:
  Opens key:
                                        HKCU\software\classes\.htm\shellex\{000214e6-0000-0000-c000-
00000000046}
  Opens key:
                                        HKCR\.htm\shellex\{000214e6-0000-0000-c000-00000000046}
  Opens key:
                                        HKCU \setminus software \setminus classes \setminus system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap shellex \cap shellex \setminus \{000214e6-text\} \cap shellex \cap 
0000-0000-c000-000000000046}
                                       Opens key:
000000000046}
  Opens key:
                                        HKCU\software\classes\*\shellex\{000214e6-0000-0000-c000-000000000046}
                                        HKCR\*\shellex\{000214e6-0000-0000-c000-00000000046}
  Opens key:
  Opens key:
                                        HKCU\software\classes\protocols\name-space handler\file\
                                        HKCR\protocols\name-space handler\file
  Opens kev:
  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
                                       HKCU\software\microsoft\internet
  Opens key:
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
  Opens key:
                                        HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:
                                        HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
  Opens key:
                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
  Opens key:
                                        HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\treatas
                                        HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32
                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserverx86
                                        HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserverx86
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\localserver32
                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver32
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler32
                                        HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\ \ liprochandler 32
  Opens key:
                                        HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
  Opens key:
00aa003f8646}\inprochandlerx86
                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandlerx86
  Opens key:
  Opens key:
                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\localserver
  Opens key:
                                       HKCR \ clsid \ \{275c23e2-3747-11d0-9fea-00aa003f8646\} \ local server
```

```
HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\}
           Opens key:
           Opens key:
                                                                                                                                                               HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
                                                                                                                                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560-c2a7-11cf-bff4-444553540000\} \setminus shell \in Classes \setminus clsid \setminus cl
           Opens key:
                                                                                                                                                               HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell
           Opens key:
                                                                                                                                                              HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c
           Opens kev:
 444553540000}\shellex\iconhandler
                                                                                                                                                               \label{lem:hkcr} \label{lem:hkcr} HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\\\ \label{lem:hkcr} \label{lem:hkcr} \label{lem:hkcr}
           Opens key:
                                                                                                                                                               \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \ff 393560-c2a 7-11cf-bff 4-444553540000 \clsid \end{tabular} \\ \begin{tabular}{ll} CU \software \classes \clsid \ff 393560-c2a 7-11cf-bff 4-444553540000 \clsid \end{tabular} \\ \begin{tabular}{ll} CU \software \clsid \cls
           Opens key:
                                                                                                                                                               HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid
           Opens key:
           Opens key:
                                                                                                                                                              HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\inprocserver32
           Opens key:
                                                                                                                                                               \label{lem:hkcrclsid} $$HKCR\clsid{ff393560-c2a7-11cf-bff4-444553540000}\nprocserver32$
           Opens key:
                                                                                                                                                               HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\treatas
           Opens key:
                                                                                                                                                               HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\
           Opens key:
                                                                                                                                                               HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\inprocserverx86
           Opens key:
                                                                                                                                                               HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserverx86
           Opens key:
                                                                                                                                                               HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\localserver32
           Opens key:
                                                                                                                                                               HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32
           Opens key:
                                                                                                                                                               HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\inprochandler32
           Opens key:
                                                                                                                                                               HKCR\clsid\ff393560-c2a7-11cf-bff4-444553540000\normalcolline{32}
           Opens key:
                                                                                                                                                               HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandlerx86
           Opens key:
                                                                                                                                                               Opens key:
                                                                                                                                                              HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\localserver
           Opens key:
                                                                                                                                                               HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver
           Opens key:
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ objects \ \ \{ff393560-c2a7-11cf-mail \ new \
bff4-444553540000}
           Opens key:
                                                                                                                                                               HKCU\software\microsoft\windows\currentversion\internet
  settings\5.0\cache\extensible cache\mshist012016042820160429
           Opens key:
                                                                                                                                                               \label{lem:hkcu} \verb+KKCU\+ software\+ internet explorer\+ main\+ windows search
           Opens key:
                                                                                                                                                               HKLM\software\policies\microsoft\internet explorer\feeds
           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
                                                                                                                                                              HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
           Opens key:
 08002b30309d}\shellfolder
                                                                                                                                                               HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
           Opens key:
                                                                                                                                                              HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-texplorer\} \setminus \{20d04fe0-te
           Opens key:
  3aea-1069-a2d8-08002b30309d}
           Opens kev:
                                                                                                                                                               HKCU\software\microsoft\windows\currentversion\policies\nonenum
           Opens key:
                                                                                                                                                               HKLM\software\microsoft\windows\currentversion\policies\nonenum
                                                                                                                                                               HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta, for explorer \setminus clsid \setminus \{20d04f
           Opens key:
 3aea-1069-a2d8-08002b30309d}\shellfolder
                                                                                                                                                              HKLM \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-delta \ explorer \ ex
           Opens key:
  3aea-1069-a2d8-08002b30309d}\shellfolder
           Opens kev:
                                                                                                                                                              HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
                                                                                                                                                               HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
           Opens key:
           Opens key:
                                                                                                                                                               HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\
           Opens key:
                                                                                                                                                               HKCU\software\microsoft\windows\shellnoroam
                                                                                                                                                               HKCU\software\microsoft\windows\shellnoroam\muicache
           Opens key:
           Opens key:
                                                                                                                                                               HKCU\software\microsoft\windows\shellnoroam\muicache\
           Opens key:
                                                                                                                                                               c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                                                               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
           Opens key:
  77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                                                               HKLM \setminus software \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus irrosoft \setminus ir
           Opens key:
  e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
          Opens key:
                                                                                                                                                              HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
 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
0 f816 c09 f4ee \\ \\ \\ category \\ \\ item \\ \\ \{a48 fa74 e-f767-44 e4-bfbc-169 e8 b38 ff58\} \\
           Queries value:
                                                                                                                                                              HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
           Queries value:
                                                                                                                                                              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
           Oueries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
           Queries value:
                                                                                                                                                              HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
           Queries value:
                                                                                                                                                              HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[bdc27c485a35c61c7bf0bfedbf9b0b3f]
```

compatibility[bdc27c485a35c61c7bf0bfedbf9b0b3f] Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls] Oueries value:

HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]

HKLM\software\microsoft\windows nt\currentversion\ime

Queries value: HKLM\system\setup[systemsetupinprogress]

Oueries value:

```
Oueries value:
                                                   HKCU\control panel\desktop[multiuilanguageid]
   Oueries value:
                                                   HKCU\control panel\desktop[smoothscroll]
   Oueries value:
\label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[enableballoontips]| \\
   Oueries value:
                                                  HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
   Oueries value:
                                                  HKLM\software\microsoft\ole[rwlockresourcetimeout]
                                                  HKCR\interface[interfacehelperdisableall]
   Oueries value:
   Oueries value:
                                                  HKCR\interface[interfacehelperdisableallforole32]
   Oueries value:
                                                   HKCR\interface[interfacehelperdisabletypelib]
                                                  HKCR\interface\{00020400-0000-0000-c000-
   Oueries value:
00000000046}[interfacehelperdisableall]
   Oueries value:
                                                  HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableallforole32]
   Queries value:
                                                   HKLM\software\microsoft\ctf\systemshared[cuas]
   Queries value:
                                                   HKCU\keyboard layout\toggle[language hotkey]
                                                   HKCU\keyboard layout\toggle[hotkey]
   Oueries value:
   Queries value:
                                                   HKCU\keyboard layout\toggle[layout hotkey]
   Queries value:
                                                   HKLM\software\microsoft\ctf[enableanchorcontext]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ policies \ \ explorer [no control panel]
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
                                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
   Queries value:
                                                   HKLM\system\wpa\pnp[seed]
   Queries value:
   Queries value:
                                                   HKLM\system\setup[osloaderpath]
   Oueries value:
                                                   HKLM\system\setup[systempartition]
                                                   HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:
   Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
   Oueries value:
                                                  HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
                                                   HKLM\software\microsoft\windows\currentversion[devicepath]
   Queries value:
   Oueries value:
                                                   HKLM\software\microsoft\windows\currentversion\setup[loglevel]
   Oueries value:
                                                  HKLM\software\microsoft\windows\currentversion\setup[logpath]
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Queries value:
                                                   HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:
                                                   HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
                                                   HKLM\software\microsoft\rpc[maxrpcsize]
   Oueries value:
   Queries value:
11e3-9fc7-806d6172696f}[data]
   Oueries value:
HKCU \ software \ icrosoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-five \ for \ f
11e3-9fc7-806d6172696f}[generation]
   Queries value:
                                                   HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                                                   HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ policies \ \ explorer \ [force active desk to pon]
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{l}{l}{HKCU \software \mbox{$microsoft \windows \current version \policies \explorer[classicshell]]} \end{tabular}
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
   Queries value:
                                                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidden \cite{tabular} \end{tabular}
   Oueries value:
HKCU \ software \ \verb|microsoft| windows \ \verb|currentversion| explorer \ | advanced [showcompcolor] | the software \ | advanced \ | adva
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value:
```

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} showing tip \cite{tabular} and \cite{$

Oueries value:

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]

Oueries value:

Queries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [separate process]$

Queries value:

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

Queries value: HKCR\directory[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]

Queries value: HKLM\software\clients\startmenuinternet[]

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

settings[disableimprovedzonecheck]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-

ab78-1084642581fb]

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

0000-0000000000000]

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

manager[safeprocesssearchmode]

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

manager\appcompatibility[disableappcompat]

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

Queries value:

 $\label{lem:hklmsoftware policies microsoft windows safer code identifiers [authentic ode enabled] \\$

 $Queries\ value: \\ HKLM\ software\ policies\ microsoft\ windows\ safer\ code identifiers [levels]$

Queries value:

Queries value:

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

Queries value:

Queries value:

Queries value:

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

Queries value:

Queries value:

Queries value:

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

Queries value

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

Queries value:

Queries value:

```
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-644445-8411-644445-8411-644445-8411-64446-8411-64446-8411-64446-8411-64446-8411-64446-8411-64446-84446-84446-84446-84446-84446-84446-84446-8446-8446-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-8446668-844666-84466-844666-84466-844666-844666-84466-84466-844666-844666-84466-84466-844668-846666
085bcc18a68d}[hashalg]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
  Queries value:
b91490411bfc}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
  Queries value:
b91490411bfc}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
                                       HKCU\software\microsoft\windows\currentversion\explorer\shell
  Queries value:
folders[cache]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
                                       HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32 [bi]
  Oueries value:
                                        HKLM\software\microsoft\windows nt\currentversion\ime compatibility[bi]
  Queries value:
                                       HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_protocol_lockdown[bi.exe]
                                        HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:
  Queries value:
                                        HKCU\software\microsoft\ctf[disable thread input manager]
  Oueries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[secureprotocols]
                                        HKLM\software\policies\microsoft\internet
  Queries value:
explorer\main[security_hklm_only]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablekeepalive]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[cachemode]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablenegotiate]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
  Queries value:
                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                       HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                       \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[clientauthbuiltinui]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                                        HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  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[signature]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
                                       HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[cachelimit]
  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}.
```

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

settings\5.0\cache\cookies[peruseritem]

Queries value:

```
settings\5.0\cache\cookies[peruseritem]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[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\cookies[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[peruseritem]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
                          \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}.
 Oueries value:
settings\5.0\cache\history[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 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
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[serverinfotimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirytimesecs]
                            HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature disable unicode handle closing callback[bi.exe]
 Queries value:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablent4rascheck]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[dialupuselansettings]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[bypassftptimecheck]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
```

```
settings[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
  Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  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[wpadsearchalldomains]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablelegacypreauthasserver]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  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[bypasshttpnocachecheck]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bvpasssslnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                            HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                            HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sharecredswithwinhttp]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[mimeexclusionlistforcache]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[headerexclusionlistforcache]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheenabled]
                           \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}.
  Oueries value:
settings[dnscacheentries]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscachetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonpost]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonzonecrossing]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[warnonbadcertsending]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpostredirect]
  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[alwaysdrainonredirect]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Oueries value:
```

Oueries value:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

 $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \catalog_entries \namespace_catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \cat$

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 [address family] \\ Queries \ value:$

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

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

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

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

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

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

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

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

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

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

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

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

 $\label{lem:hklm} \verb+Kklm/system/currentcontrolset/services/winsock2\parameters[ws2_32numhandlebuckets]$

Queries value: KLM\system\cu Queries value:

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

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

settings[globaluseroffline]

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

settings[enableautodial]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[urlencoding]

Queries value:

settings[truncatefilename]
 Oueries value: HKCU\software\microsoft\windows\currentversion\internet

Queries value: HKCU settings[badproxvexpirestime]

Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[bi.exe]
Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling[*]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Oueries 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[midil
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi61
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries 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]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Queries value:
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
  Oueries value:
                           HKLM\software\microsoft\tracing[enableconsoletracing]
                           HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
                           HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Queries value:
  Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                           HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32[filedirectory]
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[common appdata]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\winlogon[userenvdebuglevel]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\winlogon[chkaccdebuglevel]
                           HKLM\system\currentcontrolset\control\productoptions[producttype]
  Oueries value:
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}
  Queries value:
folders[local settings]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\profilelist[defaultuserprofile]
                           HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
  Queries value:
                           HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[migrateproxy]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[proxyserver]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyoverride]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[autoconfigurl]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]

Oueries value:

settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[defaultconnectionsettings] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [queryadaptername]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash dnscache \backslash parameters [registration enabled]}$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries 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: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update to plevel domain zones]$ HKLM\system\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] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]$

```
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
                                            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Oueries value:
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
   Queries value:
c7d49d7cecdc}[leaseobtainedtime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
   Queries value:
c7d49d7cecdc}[dhcpserver]
                                            HKLM\software\microsoft\internet
   Queries value:
explorer \verb|\main| featurecontrol \verb|\feature_disable_unicode_handle_closing_callback[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]|
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
   Oueries value:
c7d49d7cecdc}[disableadapterdomainname]
   Queries value:
c7d49d7cecdc}[registrationenabled]
   Oueries value:
c7d49d7cecdc}[registeradaptername]
   Oueries value:
c7d49d7cecdc}[registrationmaxaddresscount]
   Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[maxnumberofaddressestoregister]
   Queries value:
c7d49d7cecdc}[domain]
   Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[dhcpdomain]
   Queries value:
c7d49d7cecdc}[ipautoconfigurationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
   Oueries value:
c7d49d7cecdc}[dhcpnameserver]
   Oueries value:
                                            HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
   Queries value:
                                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
   Queries value:
                                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
   Queries value:
                                            HKLM\software\microsoft\rpc\securityservice[10]
   Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
   Oueries value:
   Oueries 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]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
   Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
```

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]

Queries value:

```
Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Oueries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\digest.dll[capabilities]
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
  Oueries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
                           HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msnsspc.dll[name]
  Oueries value:
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
  Queries value:
                           HKCU\software\microsoft\internet explorer\main[start page]
  Queries value:
                           HKCU\software\microsoft\internet explorer\searchscopes[defaultscope]
  Queries value:
                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[url]
  Queries value:
                           HKLM\software\microsoft\com3[com+enabled]
  Oueries value:
                           HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
  Oueries value:
                           HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
                           HKLM\system\currentcontrolset\control\session
  Queries value:
manager\environment[processor_architecture]
                           HKLM\software\microsoft\net framework setup\ndp\v2.0.50727[install]
  Oueries value:
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus framework \ setup \setminus ndp \setminus v2.0.50727[sp]
  Queries value:
                           HKLM\software\microsoft\net framework setup\ndp\v3.0[install]
  Oueries value:
                           HKLM\software\microsoft\net framework setup\ndp\v3.0[sp]
  Queries value:
                           HKLM\software\microsoft\com3[regdbversion]
  Queries value:
                           HKLM\software\microsoft\net framework setup\ndp\v3.5[install]
                           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]
  Oueries value:
                           HKCR\clsid\{8856f961-340a-11d0-a96b-
  Oueries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
  Queries value:
                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
  Oueries value:
                           HKCR\clsid\{8856f961-340a-11d0-a96b-
  Queries value:
00c04fd705a2}\inprocserver32[threadingmodel]
                           \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ app\ paths\+ iexplore.exe[]
  Queries value:
                           HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
  Queries value:
                           HKCR\interface \\ \{eab22ac1-30c1-11cf-a7eb-0000c05bae0b\} \\ typelib[]
  Oueries value:
                           HKLM\software\microsoft\internet explorer\setup[installstarted]
  Oueries value:
                           HKCR \ interface \ \{b722bccb-4e68-101b-a2bc-00aa00404770\} \ proxystubclsid32[]
                           HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
  Oueries value:
  Queries value:
                           HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[1
  Queries value:
                           HKCR \ interface \ \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \ proxystubclsid32[]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[createuricachesize]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablepunycode]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
  Oueries value:
                           HKLM\software\microsoft\internet explorer\main[navigationdelay]
                           HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\internet explorer\main[frametabwindow]
  Oueries value:
                           HKCU\software\microsoft\internet explorer\main[framemerging]
                           HKLM\software\microsoft\internet explorer\main[framemerging]
  Oueries value:
  Queries value:
                           HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Oueries value:
                           HKLM\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:
                           HKCU\software\microsoft\internet explorer\main[admintabprocs]
                           HKLM\software\microsoft\internet explorer\main[admintabprocs]
  Oueries value:
  Queries value:
                           HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
  Queries value:
                           HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:
                           HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
                           HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
  Oueries value:
  Queries value:
                           HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                           HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus shell
  Oueries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
                           HKCU\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
```

Queries value:

```
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
                                     HKLM\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions \\ \\ cached [\{871c5380-42a0-1069-a2ea-08002b30309d\} \\ \{000214e6-0000-0000-c000-0000000000046\} \\ \\ \\ \\ extensions \\ \\ \\ extensions \\ \\ extensions
0x4011
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x4011
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
  Oueries value:
  Oueries value:
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
  Oueries 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[]
  Queries value:
  Queries value:
                                     HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[appid]
                                     HKCR\clsid\{3050f3bc-98b5-11cf-bb82-
  Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
                                   HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_object_caching[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
  Queries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
                                     HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:
  Queries value:
                                     HKLM\software\microsoft\internet explorer\application
compatibility[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
                                     HKCU\software\microsoft\internet explorer\domstorage[totallimit]
  Queries value:
  Queries value:
                                     HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
  Queries value:
                                     HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
                                     HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:
  Queries value:
                                     HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                                     \label{local-observation} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\bar{\c ietld[ietlddllversionlow]}} \mbox{}
  Queries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Oueries value:
                                     HKLM\software\policies\microsoft\internet
  Oueries value:
explorer\security[disablesecuritysettingscheck]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\0[flags]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\2[flags]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[flags]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
  Oueries value:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
                                     HKCU\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
                                     HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[specialfolderscachesize]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer[no3dborder]
  Queries value:
                                     HKLM\software\microsoft\internet explorer[no3dborder]
                                     HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:
  Oueries value:
                                     HKCR\.htm[content type]
  Oueries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
  Oueries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
```

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

settings[istextplainhonored]

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_safe_bindtoobject[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]

Oueries value: 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[] Oueries value:

HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid] Oueries value:

Oueries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserver32[threadingmodel]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrollinset]

Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrolldelay] HKCU\software\microsoft\windows Oueries value: nt\currentversion\windows[dragscrollinterval]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_restrict_filedownload[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[*] Oueries value: HKCR\protocols\handler\about[clsid] Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[inprocserver32]

HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[] Oueries value:

Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]

Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[threadingmodel]

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

manager[pendingfilerenameoperations2]

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

manager[pendingfilerenameoperations]

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

settings\zones\3[2106]

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

settings\zones\3[2106]

HKCU\software\microsoft\internet explorer\zoom[zoomdisabled] Oueries value: Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[] Queries value: HKLM\software\policies\microsoft\internet explorer[smartdithering] Oueries value: HKCU\software\microsoft\internet explorer[smartdithering] HKCU\software\microsoft\internet explorer[rtfconverterflags] Queries value: HKLM\software\policies\microsoft\internet explorer\main[usecleartype] Oueries value:

HKCU\software\microsoft\internet explorer\main[usecleartype] Oueries value:

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

explorer\main[page_transitions]

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

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

explorer\main[use_dlgbox_colors]

HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] Queries value: Queries value: HKLM\software\policies\microsoft\internet explorer\main[anchor underline]

HKCU\software\microsoft\internet explorer\main[anchor underline] Oueries value: HKCU\software\microsoft\internet explorer\main[css_compat] Queries value: Oueries value: HKCU\software\microsoft\internet explorer\main[expand alt text] Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline

images]

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

videos]

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

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

explorer\main[play_background_sounds]

Queries value: HKCU\software\microsoft\internet explorer\main[play_background_sounds] Oueries value: $HKLM \setminus software \setminus policies \setminus microsoft \setminus internet \ explorer \setminus main[play_animations]$

HKCU\software\microsoft\internet explorer\main[play_animations] Oueries value:

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] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll] Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[xmlhttp] Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp] Queries value: HKLM\software\policies\microsoft\internet explorer\main[show image

placeholders1

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

debugger]

HKCU\software\microsoft\internet explorer\main[disable script debugger] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie] HKCU\software\microsoft\internet explorer\main[move system caret] Oueries value: Queries value: $\label{lem:hkcu} \verb+KKCU\+ software\+ internet explorer\+ main[force offscreen]$

```
composition]
```

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

autoimageresize]

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

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

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

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

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

Oueries value:

explorer\international[default_codepage]

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

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

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

size]

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

face]

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

hyperlinks]

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

color]

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

programmatic cut_copy_paste]

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

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

HKCU\software\microsoft\internet Oueries value:

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

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

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

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

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zone_elevation[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]

Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[*]

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

settings\zones\0[2700]

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

settings\zones\0[2700]

HKLM\software\microsoft\internet Oueries value:

explorer\main\featurecontrol\feature_xssfilter[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]

HKLM\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_xssfilter[*]

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

settings\zones[securitysafe]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nofileurl] HKCU\software\microsoft\windows\currentversion\internet Queries value:

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]

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

settings[cointernetcombineiuricachesize]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_subdownload_lockdown[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]

Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown[*]

Queries value: HKCR\.css[content type] Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_behaviors[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]

HKLM\software\microsoft\internet Oueries value:

explorer\main\featurecontrol\feature_behaviors[*]

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

settings\zones\0[2000]

HKLM\software\microsoft\internet explorer\default behaviors[discovery] Oueries value:

Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-

```
00aa00bdce0b}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Oueries value:
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
                                    \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} \label{thm:local_hammon_hammon} \end{tabular}
  Queries value:
settings\zones\0[1400]
  Oueries value:
                                    HKCR\.js[content type]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[*]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zonemap[autodetect]
  Queries value:
                                    HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
  Queries value:
                                    HKCR\clsid\{50d5107a-d278-4871-8989-
  Queries value:
f4ceaaf59cfc}\inprocserver32[threadingmodel]
  Queries value:
                                    HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
  Queries value:
                                    HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
  Oueries value:
  Queries value:
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
  Queries value:
                                    HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-
  Queries value:
869523e2d6c7}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
  Oueries value:
  Queries value:
                                     HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
  Queries value:
                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
                                    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
  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]
                                    HKCU\software\microsoft\windows\currentversion\internet settings\url
  Oueries value:
history[daystokeep]
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
  Queries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
  Oueries value:
  Queries value:
                                     HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\0[1201]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                    HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
                                     HKLM\software\microsoft\ole[defaultaccesspermission]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
                                     HKCR\.jpg[content type]
  Oueries value:
  Queries value:
                                     HKCR\.png[content type]
  Queries value:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
  Queries value:
  Oueries value:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-
  Queries value:
00aa006c1a01}\inprocserver32[threadingmodel]
  Oueries value:
                                    HKCR\mime\database\content type\image/bmp\bits[0]
                                     HKCR\mime\database\content type\image/gif\bits[0]
  Oueries value:
  Queries value:
                                     HKCR\mime\database\content type\image/jpeg\bits[0]
                                     HKCR\mime\database\content type\image/pjpeg\bits[0]
  Queries value:
                                     HKCR\mime\database\content type\image/png\bits[0]
  Queries value:
                                     HKCR\mime\database\content type\image/x-png\bits[0]
  Oueries value:
  Oueries value:
                                     HKCR\mime\database\content type\image/x-wmf\bits[0]
  Oueries 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}\ \ inprocserver 32[]
```

Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]

Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprocserver32[threadingmodel]

Queries value: HKCU\software\microsoft\internet explorer\recovery[autorecover]

Queries value: HKCU\software\microsoft\ftp[use web based ftp]

Queries value: HKCU\software\microsoft\internet

explorer\services[selectionactivitybuttondisable]

Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]
Queries value: HKLM\software\microsoft\internet explorer\feed discovery[sound]

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

settings\zones\3[2700]

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

settings\zones\3[2700]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[compatible]

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

settings\5.0\user agent[compatible]

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

settings\5.0\user agent[version]

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

settings\5.0\user agent[version]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user

agent]

Queries 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]

Queries value: HKLM\software\microsoft\internet

 $explorer \verb|\main| feature_max connections perserver [bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]|$

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver[*] Queries value: HKLM\software\microsoft\internet

 $explorer \verb|\main| featurecontrol \verb|\feature| max connection sper 1_0 server [bdc 27c485a 35c61c7bf 0bfedbf 9b 0b3f.exe]|$

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*] Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]

Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[appid]

Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserver32[threadingmodel]

 $\label{thm:constraint} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$

settings\zones\3[1a10]

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

Queries value: HKCU\software\microsoft\internet explorer\main[friendly http errors]

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

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

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

 Queries value:
 HKLM\system\currentcontrolset\control\windows[csdversion]

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

settings\zones\3[currentlevel]

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

folders[local appdata]

Queries value:

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

Queries value:

Queries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|.htm[application] | the limit of the limit of$

Oueries value: HKCR\.htm[]

Queries value: HKCR\htmlfile\shellex\iconhandler[]

Queries value: HKCR\htmlfile[docobject]
Queries value: HKCR\.htm[perceivedtype]

Queries value: HKCR\systemfileassociations\text[docobject]

Queries value: HKCR\htmlfile[browseinplace]

Queries value: HKCR\systemfileassociations\text[browseinplace]

Queries value: HKCR\htmlfile\clsid[]
Queries value: HKCR\htmlfile[isshortcut]

Queries value: HKCR\systemfileassociations\text[isshortcut]

Queries value: HKCR\htmlfile[alwaysshowext]

Queries value: HKCR\systemfileassociations\text[alwaysshowext]

Oueries value: HKCR\htmlfile[nevershowext]

Queries value: HKCR\systemfileassociations\text[nevershowext]

Queries value: HKCU\appevents\schemes\apps\explorer\navigating\.current[]

Oueries value: HKCU\seftware\microsoft\windows\currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\explorer\userschlarg\.currentversion\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg\.current\userschlarg

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

folders[recent]

Queries 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]
                                            HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
   Oueries value:
                                             HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[appid]
   Queries value:
   Queries value:
                                             HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[threadingmodel]
   Queries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[1250]
                                             HKLM\system\currentcontrolset\control\nls\codepage[1251]
   Oueries value:
   Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[1253]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[1254]
                                             HKLM\system\currentcontrolset\control\nls\codepage[1255]
   Oueries value:
   Oueries 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]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[874]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[932]
                                             HKLM\system\currentcontrolset\control\nls\codepage[936]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[949]
   Oueries value:
   Queries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[1361]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobiect1
   Oueries value:
   Queries value:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[browseinplace]
   Queries value:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}\[isshortcut]
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[alwaysshowext]
   Oueries value:
   Queries value:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}[nevershowext]
   Queries value:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-
   Oueries value:
444553540000}\inprocserver32[loadwithoutcom]
   Queries value:
                                            HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
                                             HKCU\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
                                            HKLM\software\microsoft\windows\currentversion\shell
   Oueries value:
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x401]
                                            HKCU\software\microsoft\windows\currentversion\shell
   Oueries value:
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x401]
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-
   Oueries value:
444553540000}\inprocserver32[inprocserver32]
   Queries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-}
444553540000}\inprocserver32[threadingmodel]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix]
                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit]
                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions]
   Queries value:
                                            HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
   Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
   Queries value:
                                             HKCR\.url\persistenthandler[]
   Queries value:
                                             HKLM\software\microsoft\windows search[currentversion]
   Oueries value:
                                            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
   Queries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
   Oueries value:
08002b30309d}1
   Queries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
   Oueries value:
                                            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \
   Oueries value:
1757981266-507921405-1957994488-1003[userpreference]
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Oueries value:
1757981266-507921405-1957994488-1003[centralprofile]
                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and \end{tabular} in the current version \end{tabular} and \end{tabular} and \end{tabular} in the current version \end{tabular} and \end
   Oueries value:
1757981266-507921405-1957994488-1003[profileloadtimelow]
```

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

1757981266-507921405-1957994488-1003[profileloadtimehigh]

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

Queries value:

 $HKCU \ software \ microsoft \ windows \ system 32 \ shell 32. dll, -9216]$ Queries value: HKLM\software\microsoft\internet explorer\main[maxrenderline]

HKCU\software\appdatalow\software\smartbar[globaluserid] Sets/Creates value:

HKLM\system\currentcontrolset\control\session Sets/Creates value:

manager[pendingfilerenameoperations]

Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[offerid] 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\software\conduit\distributionengine\1\offerhistory\755131[defaultsearch]

Sets/Creates value:

HKCU\software\conduit\distributionengine\1\offerhistory\755131[offerdescription]

Sets/Creates value:

Sets/Creates value:

HKCU\software\conduit\distributionengine\1\offerhistory\755131[rootofferid] HKCU\software\microsoft\windows\currentversion\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] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit]

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: 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:

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

folders[history] Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common appdata]

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

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname] HKCU\software\microsoft\windows\currentversion\internet Value changes:

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect] HKCU\software\microsoft\windows\currentversion\explorer\shell

Value changes:

folders[local appdata]

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

settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]

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

folders[favorites]

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

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

manager[pendingfilerenameoperations]