Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 188, Task ID: 751

Task ID: 751 Risk Level:

Date Processed: 2016-04-28 13:08:09 (UTC)

Processing Time: 61.08 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\f4cade5dce24d5c9d966cb266c7c7346.exe"

Sample ID: Type: Owner: admin

f4cade5dce24d5c9d966cb266c7c7346 Label:

Date Added: 2016-04-28 12:45:09 (UTC) PE32:win32:gui File Type:

File Size: 994648 bytes

f4cade5dce24d5c9d966cb266c7c7346 MD5:

cd219ea43a5ea45c6a471857bcf0344f7c50c5eed41b8323ce6e92f5a0ccee49 SHA256:

Description: None

Pattern Matching Results

5 Creates process in suspicious location

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]

3 Long sleep detected

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\f4cade5dce24d5c9d966cb266c7c7346.exe
["c:\windows\temp\f4cade5dce24d5c9d966cb266c7c7346.exe"]
                                        C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\BI.exe { "json_send_time" : "28/4/2016 15:8:36:347" , "product_id_version" : "" , "product_type" : "" , "product_id" : "" , "offer_id" : "167312" , "user_type" : "NULL" , "result" : "Success" , "user_operating_system_bits" : "" , "current_default_search" : "" , "current_homepage" : "" , "current_toolbars" : "" ,
"attempt_number": "1", "is_silent": "", "user_ms_dotnet_framework_ver": "",

"user_acount_type": "", "user_ie_version": "", "user_default_browser_version": "",

"user_default_browser": "", "user_service_pack": "", "user_operating_system": "",

"revision_number": "0", "build_id": "00000000", "dm_version": "1.3.7.9_NoStatic.130521.01",

"bundle_id": "8c319a0a-ba3c-4eb9-8259-f1009d9bf345", "machine_user_id": "{COD2C7DB-0178-4771-
B076-E595C1B5E480}" , "send_attempt" : "0" , "channel_id" : "" , "installation_session_id" :
"2E19C248-CEF0-4257-A3BA-1D1726545A83" , "publisher_internal_id" : "1" , "publisher_id" : "Brothersoft" , "publisher_account_id" : "Brothersoft" , "order" : "1.0" , "phase" : "Init" , "Is_Test" : "0" }]
  Creates process:
                                          C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\BI.exe { "user_ie_security_level" : "Unknown-0"
"json_send_time" : "28/4/2016 15:9:48:13" , "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/167253/?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": "167312", "general_status_code": "6", "duration_details": " InitPluginsDir:0
initializeParams:381 load BITool:190 send BI Init:231 load DownloadACC:60 retrieveUISource:10
unpack_webappfolder:0 unpack_icon:10 RetrieveMainOfferKey:0 unpack_OpenCandyDll:300
load_webapphost:0 unpack_ProxyInstaller:20 navigate_loadingUI:1742 navigateAsync_constMainOffer:0
BuildUserProfile:10 retrieve cid:0 callService1:66709 parse_ResponseXml:1062
init_external_offer:0 DiscoverUserAgent:250 " , "phase_duration" : "" , "error_details" : "55
Failed to communicate with CMS for main offer" , "result" : "Error" ,
"user_operating_system_bits" : "32" , "current_default_search" :
"http://search.live.com/results.aspx?q={searchTerms}&src=IE-SearchBox&Form=IE8SRC"
"current_homepage": "about:blank", "current_toolbars": "", "attempt_number": "1",

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

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

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

"Microsoft Windows XP", "revision_number": "0", "build_id": "000000000", "dm_version":

"11.2.7.0.NeSteric 105531.01", "burdle_id": "0020000000", "dm_version":
"1.3.7.9_NoStatic.130521.01" , "bundle_id" : "8c319a0a-ba3c-4eb9-8259-f1009d9bf345"
"machine_user_id" : "{COD2C7DB-0178-4771-B076-E595C1B5E480}" , "send_attempt" : "0"
"channel_id" : "" , "installation_session_id" : "2E19C248-CEF0-4257-A3BA-1D1726545A83"
```

```
"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\nsn3.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
                          \BaseNamedObjects\ZonesCounterMutex
 Creates mutex:
                          \BaseNamedObjects\ZoneAttributeCacheCounterMutex
 Creates mutex:
 Creates mutex:
                         \BaseNamedObjects\ZonesCacheCounterMutex
 Creates mutex:
                          \BaseNamedObjects\ZonesLockedCacheCounterMutex
                         \BaseNamedObjects\MSIMGSIZECacheMutex
 Creates mutex:
 Creates mutex:
                         \BaseNamedObjects\_!SHMSFTHISTORY!_
                         \BaseNamedObjects\c:!documents and settings!admin!local
 Creates mutex:
settings!history!history.ie5!mshist012016042820160429!
 Creates mutex:
                         \BaseNamedObjects\MSCTF.Shared.MUTEX.MPH
                          \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\OleDfRoot000021C4E
```

File Cyctom Fyente

Files\Content.IE5\UH4D6D6X\navcancl[1]

Creates semaphore:

File System Events		
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsp1.tmp	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nst2.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.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\nsn3.tmp\System.dll</pre>	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\System.dll	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsn3.tmp\webapphost.dll		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\BI.exe</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsn3.tmp\DM_loader.gif		
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsn3.tmp\DownloadACC.exe		
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\Failed.htm	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\icon.png</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsn3.tmp\OCSetupHlp.dll		
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsj4.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsx5.tmp</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp</pre>	
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsr6.tmp	
Creates:	${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsr6.tmp\linetc.dll}$	
Creates:	<pre>C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\webapphost.dll</pre>	
Creates:	C:\Documents and Settings\Admin\Local	
Settings\Temp\nsn3.tmp\ProxyInstaller.exe		
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\~DF1C51.tmp	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp\a.txt</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\inetc.dll</pre>	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\offer.xml</pre>	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temporary Internet	
Files\Content.IE5\QXMNQBKF\navcancl[1]		
Creates:	<pre>C:\DOCUME~1\Admin\LOCALS~1\Temp\nsr6.tmp\inetc.dll</pre>	
Creates:	C:\Documents and Settings\Admin\Local Settings\Temporary Internet	

```
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]
 Creates:
                         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
 Creates:
Files\Content.IE5\UH4D6D6X\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\background_gradient[2]
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\xml.dll
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\xml.dll
 Creates:
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\nsArray.dll
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\nsArray.dll
 Creates:
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_webOC[1]
                         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\info 48[2]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\down[1]
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\OXMNOBKF\down[1]
 Creates
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\UH4D6D6X\dnserrordiagoff web0C[1]
                         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\nsm7.tmp
 Creates:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nse8.tmp}
                         C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nso9.tmp
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp\inetc.dll
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp\a.txt
 Creates:
 Creates:
                         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
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nso9.tmp\inetc.dll
                         C:\Documents and Settings\Admin
 Opens:
 Opens:
                         C:\WINDOWS\svstem32\imm32.dll
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86 Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
                         C:\WINDOWS\WindowsShell.Config
 Opens:
 Opens:
                         C:\WINDOWS\Temp\f4cade5dce24d5c9d966cb266c7c7346.exe
```

```
C:\windows\temp\f4cade5dce24d5c9d966cb266c7c7346.exe.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
                         C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\COMCTL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
                         C:\WINDOWS\system32\shfolder.dll
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
 Opens:
                         C:\
                         C:\Documents and Settings
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsp1.tmp
                         C:\WINDOWS\Temp\00667005-5b79-4a13-b621-3e8b756c4979
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp
                         {\tt C:\Documents\ and\ Settings\backslash Admin\backslash Local\ Settings\backslash Temp\backslash nsn3.tmp}
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\System.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nsn3.tmp\webapphost.dll
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\webapphost.dll.2.Manifest
 Opens:
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\webapphost.dll.2.Config
 Opens:
                         C:\WINDOWS\system32\winspool.drv
 Opens:
                         C:\WINDOWS\system32\oledlg.dll
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\msasn1.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\oleacc.dll
 Opens:
                         C:\WINDOWS\system32\msvcp60.dll
 Opens:
                         C:\WINDOWS\system32\oleaccrc.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\webapphost.dll.1000.Manifest
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsn3.tmp\BI.exe}
 Opens:
 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
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\BI.exe.Manifest
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn3.tmp\BI.exe.124.Manifest
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsj4.tmp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp\inetc.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\Fonts\sserife.fon
 Opens:
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\asycfilt.dll
 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
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\inetc.dll
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
                         C:\WINDOWS\system32\ras
 Opens:
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk\
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
 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
```

```
C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\icon.png
 Opens:
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
 Opens:
                         C:\WINDOWS
                         C:\WINDOWS\svstem32
 Opens:
 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]
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\psapi.dll
 Opens:
                         C:\WINDOWS\system32\mlang.dll
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp\a.txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\navcancl[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\navcancl[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         C:\WINDOWS\system32\iepeers.dll
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Manifest
 Opens:
                         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:\DOCUME~1\Admin\LOCALS~1\Temp\nsr6.tmp\
                         C:\WINDOWS\system32\jscript.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[1]
 Opens:
                         C:\WINDOWS\system32\imgutil.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\0XMNOBKF\bullet[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                         C:\WINDOWS\system32\pngfilt.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[1]
 Opens:
                         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
 Opens:
Files\Content.IE5\UH4D6D6X\bullet[1]
                         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:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
                         C:\WINDOWS\Fonts\SEGOEUI.TTF
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\xml.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\offer.xml
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\nsArray.dll
                         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]
                         {\tt C:\Documents\ and\ Settings\backslash Admin\backslash Local\ Settings\backslash Temporary\ Internet}
 Opens:
Files\Content.IE5\CXCXW1MR\dnserrordiagoff_web0C[1]
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[2]
 Opens:
                         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
 Opens:
Files\Content.IE5\UH4D6D6X\down[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[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\down[2]
 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\ErrorPageTemplate[1]
                         C:\WINDOWS\Prefetch\BI.EXE-33DDD16F.pf
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsn3.tmp\Failed.htm}
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsm7.tmp
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
                         C:\WINDOWS\Fonts\arialbd.ttf
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nso9.tmp\netc.dll}
 Opens:
                         C:\WINDOWS\Fonts\verdana.ttf
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014033120140407
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings \verb|\History\History.IE5\MSHist012014033120140407 \verb|\index.dat| \\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014041220140413
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings \verb|\History\History.IE5\MSHist012014041220140413\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429
                         C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp\a.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012016042820160429\index.dat
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\nso9.tmp\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nst2.tmp
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\System.dll
 Writes to:
                         {\tt C:\Documents\ and\ Settings\Admin\Local}
 Writes to:
Settings\Temp\nsn3.tmp\webapphost.dll
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\BI.exe
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\nsn3.tmp\DM_loader.gif
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\nsn3.tmp\DownloadACC.exe
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\Failed.htm
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\icon.png
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsx5.tmp
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nsn3.tmp\OCSetupHlp.dll
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp\inetc.dll
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\nsn3.tmp\ProxyInstaller.exe
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\inetc.dll
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\navcancl[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[1]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info 48[2]
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
```

```
Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\info_48[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[2]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\bullet[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\background_gradient[2]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\offer.xml
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\xml.dll
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\nsArray.dl1
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\| Content.IE5 \verb|\| QXMNQBKF \verb|\| dnserrordiagoff\_webOC[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\dnserrordiagoff_web0C[1]
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Writes to:
Files\Content.IE5\QXMNQBKF\info_48[2]
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Writes to:
Files\Content.IE5\UH4D6D6X\down[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\bullet[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\down[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_web0C[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse8.tmp
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nso9.tmp\netc.dll}
 Writes to:
 Writes to:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
                          C:\WINDOWS\Temp\f4cade5dce24d5c9d966cb266c7c7346.exe
 Reads from:
 Reads from:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nst2.tmp}
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\BI.exe
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsx5.tmp
 Reads from:
                          C:\AUTOEXEC.BAT
                          C:\WINDOWS\Registration\R00000000007.clb
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\drivers\etc\hosts
 Reads from:
                          C:\WINDOWS\system32\rsaenh.dll
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\offer.xml
 Reads from:
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp\Failed.htm
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nse8.tmp
                          C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsp1.tmp
 Deletes:
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsn3.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsj4.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[2]
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp\a.txt
 Deletes:
 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]
 Deletes:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsr6.tmp\inetc.dll
 Deletes:
 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]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\UH4D6D6X\info_48[1]
```

```
Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
 Deletes:
                          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
 Deletes:
Files\Content.IE5\UH4D6D6X\info_48[2]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bullet[1]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\UH4D6D6X\bullet[2]
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\| Content.IE5 \verb|\| QXMNQBKF \verb|\| httpErrorPagesScripts[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\dnserrordiagoff_web0C[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\QXMNQBKF\background_gradient[2]
                          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\UH4D6D6X\down[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\bullet[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\down[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\QXMNQBKF\down[2]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Deletes:
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
                          C:\Documents and Settings\Admin\Local Settings\Temp\nsm7.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp
 Deletes:
 Deletes:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
 Deletes:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
                          C:\Documents and Settings\Admin\Local
 Deletes:
Settings\History\History.IE5\MSHist012014041220140413\index.dat
 Deletes:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
```

C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp\a.txt Deletes: Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nso9.tmp\inetc.dll

Network Events

DNS query:

DNS query: offering.service.distributionengine.conduit-services.com DNS query: cms.distributionengine.conduit-services.com offering.service.distributionengine.ams.conduit-services.com \Rightarrow DNS response: 195.78.120.173 Connects to: 195.78.120.173:80 Connects to: 127.0.0.1:1043 Sends data to: 8.8.8.8:53 offering.service.distributionengine.ams.conduit-services.com:80 Sends data to: (195.78.120.173) Receives data from: Receives data from: offering.service.distributionengine.ams.conduit-services.com:80 (195.78.120.173)

Windows Registry Events

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

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

ude.conduit-data.com

Creates key: HKCU\software

Creates key: HKCU\software\appdatalow

Creates key: HKCU\software\appdatalow\software

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

folders

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

Creates key: HKLM\software\microsoft\tracing

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

folders

Creates kev: HKCU\software\microsoft\windows nt\currentversion\winlogon Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders

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

settings\connections

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

awareness

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

Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked HKCU\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: Creates key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \begin{tabular}{ll} software \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \begin{tabular}{ll} carrent version \begin{tabular}{ll} software \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \begin{tabular}{ll} carrent version \begin{tabular}{ll} software \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \begin{tabular}{ll} carrent version \begi$ Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached

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

Creates key: $HKCU \ software \ \verb|\conduit\| distribution engine \verb|\1 \| offerhistory \| 755131$

Creates key: HKCU\software\conduit

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

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

settings\5.0\cache\extensible cache\mshist012016042820160429

Creates key: HKCU\software\microsoft\internet explorer\main\windowssearch Deletes 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[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\f4cade5dce24d5c9d966cb266c7c7346.exe

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

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

options\gdi32.dll

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

options\user32.dll

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

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ Opens key: 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: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$

options\kernel32.dll

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

options\secur32.dll

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

options\rpcrt4.dll

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

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

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

Opens key:

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: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens kev: HKLM\software\microsoft\windows\currentversion\explorer\performance

Opens key: HKLM\system\setup

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

Opens key:

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

Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \mbox{\tt advanced}$ $\label{thm:language} \mbox{HKLM\software\mbox{$\mbox{$\mbox{$\rm m$icrosoft\windows}$} nt\current version\languagepack}} \label{thm:languagepack}$ Opens key:

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\f4cade5dce24d5c9d966cb266c7c7346.exe

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

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

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

options\shfolder.dll

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

Opens key:

a2d8-08002b30309d}

Opens key: HKCU\software\classes\

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

08002b30309d}\inprocserver32

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

options\setupapi.dll

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

HKLM\system\wpa\pnp Opens key:

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

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

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

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

Opens key: HKLM\software\microsoft\rpc

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

options\f4cade5dce24d5c9d966cb266c7c7346.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 kev:

 $HKCU \ software \ icrosoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-five \ for \ f$

11e3-9fc7-806d6172696f}\

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

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 kev:

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

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

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

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

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

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

HKCU\software\classes\folder Opens key:

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

HKCR\folder\clsid Opens key:

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

options\system.dll

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

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

options\comdlg32.dll

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

options\winspool.drv

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

options\oledlg.dll

Opens key: HKCU\software\classes\clsid

Opens key: HKCR\clsid

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

options\oleaut32.dll

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

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

options\msasn1.dll

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

options\crypt32.dll

Opens key: HKLM\system\currentcontrolset\services\crypt32\performance Opens kev: HKLM\software\microsoft\windows nt\currentversion\msasn1

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

options\msvcp60.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\oleacc.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\urlmon.dll Opens key: HKCU\software\classes\protocols\name-space handler\ HKCR\protocols\name-space handler Opens key: Opens key: HKCU\software\classes\protocols\name-space handler Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\ Opens key: $\label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ main \+ feature control$ HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \label{lem:hkcu} internet explorer \main \feature control \end{tabular}$ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ $\label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\notation{ \columnwidth}{linear to the color of the color of$ Opens key: settings\zonemap\domains\ Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zonemap\ranges\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\internet Opens key: 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: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\webapphost.dll HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens kev: 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 HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\bi.exe HKLM\software\policies\microsoft\windows\safer\levelobjects Opens key: Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths$ Opens key: be2efd2c1a33} Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: edd5fbde1328} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91} Opens key: 7c29ddecae3f} Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-1441\} + (1996-1998) + (1$ 085bcc18a68d} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc} Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$

Opens key:

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

Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ has hes$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens kev: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens kev: $HKLM \ software \ \verb|\microsoft| windows \ safer \ code identifiers \ of the latter \ of th$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens kev: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$ HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key: $HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 65536 \ has hes$ Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} indows \current version \explorer \shell folders} \end{tabular}$ Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\bi.exe Opens key: HKLM\software\microsoft\ctf\compatibility\bi.exe HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\bi.exe\rpcthreadpoolthrottle Opens key: HKCU\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies HKCU\software\policies Opens key: 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 HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\content HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\content HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\cookies Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies HKCU\software\microsoft\windows\currentversion\internet Opens kev:

HKLM\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history

settings\5.0\cache\history

settings\5.0\cache\extensible cache

settings\5.0\cache\extensible cache\domstore

Opens key:

Opens key:

Opens kev:

```
Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\iecompat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\ietld
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens kev:
options\inetc.dll
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature bufferbreaking 818408
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\imm
 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
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\msctfime.ime
 Opens key:
                         HKCU\software\microsoft\ctf
                         HKLM\software\microsoft\ctf\systemshared
 Opens kev:
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKLM\software\microsoft\internet
 Opens key:
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
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\microsoft\internet
 Opens kev:
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 kev:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
 Opens key:
                         HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
```

Opens key:

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog\_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011
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
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:
                                HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                                HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens kev:
                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens kev:
                                HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:
                                \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} soft \end{tabular} windows \end{tabular} in terms to setting shift parallel soft \end{tabular} and the setting shift \end{ta
filters\rpa
 Opens key:
                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:
                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
                                HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_mime_handling
                                HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\asycfilt.dll
  Opens key:
                                HKCU\software\microsoft\internet explorer\main
  Opens key:
                                HKCU\software\microsoft\internet explorer\searchscopes
  Opens key:
                                HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}
                                HKLM\system\currentcontrolset\control\session manager\environment
  Opens key:
                                HKLM\software\microsoft\internet explorer\toolbar
  Opens kev:
  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
  Opens key:
                                HKLM\software\microsoft\windows nt\currentversion\image file execution
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:
                                HKLM\software\microsoft\net framework setup\ndp
  Opens key:
                                HKLM \ software \ microsoft \ net framework setup \ ndp \ v2.0.50727
  Opens key:
                                HKLM\software\microsoft\net framework setup\ndp\v3.0
  Opens key:
                                HKLM\software\microsoft\net framework setup\ndp\v3.5
  Opens key:
                                HKLM\software\microsoft\windows nt\currentversion
                                HKCU\software\conduit\distributionengine\1\offerhistory
  Opens kev:
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
```

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

Opens key: options\tapi32.dll

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

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

options\rasapi32.dll

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

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

options\userenv.dll

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

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

folders

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

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

Opens key: HKU\

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

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

HKCU\volatile environment Opens key: Opens key: HKLM\software\microsoft\com3

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

options\sensapi.dll

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

options\comres.dll

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

options\clbcatq.dll

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

Opens key: HKLM\software\classes

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

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

00c04fd705a2}\treatas

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

00c04fd705a2}\inprocserver32

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

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

00c04fd705a2}\inprocserverx86

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

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

00c04fd705a2}\localserver32

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

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

00c04fd705a2}\inprochandler32

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

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

00c04fd705a2}\inprochandlerx86

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86 Opens kev:

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

00c04fd705a2}\localserver

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

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

options\mswsock.dll

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

options\rasadhlp.dll

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

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

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

0000c05bae0b}\typelib

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

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

 $\label{local-continuity} HKCU \setminus software \setminus classes \setminus interface \setminus \{79 eac9c4 - baf9 - 11 ce - 8c82 - baf9 - baf$ Opens key:

00aa004ba90b}\proxystubclsid32

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

00000000046}\proxystubclsid32

Opens key:

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

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

00c04f79abd1}\proxystubclsid32

Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dnsapi.dll

Opens key:

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

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

options\iphlpapi.dll

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

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces

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

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-abe3-430-abe3-4$

c7d49d7cecdc}

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

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

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

Opens key:

a2ea-08002b30309d}

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

08002b30309d}\inprocserver32

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

Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKLM\system\currentcontrol\securityproviders
Opens key: HKLM\system\currentcontrol\set\control\lsa\sspicache

Opens key: HKLM\system\currentcontrol\sa\sspicache\msapsspc.dll
Opens key: HKLM\system\currentcontrol\sa\sspicache\digest.dll
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: $\label{eq:hccn} \begin{tabular}{ll} HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ Opens key: \\ HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid$

08002b30309d}\inprocserverx86

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

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

08002b30309d}\localserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32 Opens key: HKLM\system\currentcontrol\set\control\lsa\sspicache\msnsspc.dll

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

08002b30309d}\inprochandler32

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

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

08002b30309d}\inprochandlerx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86
Opens key: HKLM\system\currentcontrol\securityproviders\saslprofiles
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msv1_0.dll

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

08002b30309d}\localserver

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

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

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

cryptographic provider

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

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

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

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

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

Opens key: HKCR\protocols\handler\res

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

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

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

00aa00bdce0b}\treatas

Opens key: $\label{eq:hkkcr} \begin{tabular}{ll} HKCR\clsid\3050f3bc-98b5-11cf-bb82-00aa00bdce0b\treatas \\ Opens key: \\ HKCU\software\classes\clsid\3050f3bc-98b5-11cf-bb82-\\ \end{tabular}$

00aa00bdce0b}\inprocserver32

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

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

00aa00bdce0b}\inprocserverx86

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

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

00aa00bdce0b}\localserver32

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

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

00aa00bdce0b}\inprochandler32

Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32

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

00aa00bdce0b}\inprochandlerx86

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

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

00aa00bdce0b}\localserver

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

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

options\msls31.dll

```
Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mshtml.dll
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 Opens kev:
                         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
                         HKLM\software\microsoft\internet
 Opens key:
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 kev:
                         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
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_databinding_support
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enforce_bstr
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enforce_bstr
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens kev:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature object caching
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                         HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key:
 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
                         HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
 Opens key:
 Opens key:
                         HKLM\software\microsoft\internet explorer\application compatibility
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\domstorage
 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
                         HKLM\software\policies\microsoft\internet explorer\safety\privacie
 Opens key:
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\safety\privacie
                         HKCU\software\microsoft\internet explorer\safety\privacie
 Opens kev:
 Opens key:
                         HKLM\software\microsoft\internet explorer\safety\privacie
                         HKLM\software\microsoft\internet explorer\mediatypeclass
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
```

Opens key: HKCU\software\microsoft\internet

settings\accepted documents

Opens key:

explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615

HKLM\software\microsoft\windows\currentversion\policies\ratings

```
Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\protocoldefaults\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                           HKI M\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\domains\msn.com
 Opens key:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com\related
                           HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                           HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                           HKCU\software\microsoft\internet explorer\ietld
                           HKLM\software\policies\microsoft\internet explorer\security
 Opens key:
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\0
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\0
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens kev:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\3
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
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\
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 Opens key:
settings\lockdown zones\
                           \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}.
 Opens key:
settings\lockdown_zones\
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\1
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\2
 Opens key:
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
```

```
settings\lockdown_zones\2
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\3
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Soft \end{tabular} windows \current version \current versi
  Opens key:
settings\lockdown_zones\3
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
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
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
                                     HKCU\software\microsoft\internet explorer
  Opens key:
                                     HKLM\software\microsoft\internet explorer
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature restrict res to lmz
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_load_shdoclc_resources
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_load_shdoclc_resources
  Opens key:
                                     HKCU\software\classes\.htm
  Opens key:
                                     HKCR\.htm
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  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
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens kev:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key:
00aa00686f13}\treatas
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key:
00aa00686f13}\inprocserver32
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
  Opens kev:
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserverx86
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver32
  Opens kev:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key:
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
                                     HKLM\software\policies\microsoft\cryptography
  Opens key:
  Opens key:
                                     HKLM\software\microsoft\cryptography
  Opens key:
                                     HKLM\software\microsoft\cryptography\offload
                                     \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
  Opens key:
options\hnetcfg.dll
  Opens key:
                                     HKLM\svstem\currentcontrolset\services\winsock\parameters
  Opens key:
                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
                                     \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
  Opens key:
options\psapi.dll
  Opens kev:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
                                     HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature manage script circular refs
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:
                                     HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_restrict_filedownload|
```

HKLM\software\microsoft\internet explorer\security\floppy access Opens key: Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof detection HKLM\software\microsoft\internet explorer\security\adv addrbar spoof Opens key: detection Opens key: HKCU\software\classes\protocols\name-space handler\about\ HKCR\protocols\name-space handler\about Opens key: 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 kev: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

Opens key: 00aa00bdce0b}\treatas

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

00aa00bdce0b}\inprocserver32

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

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

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: $\label{eq:hkcr} \mbox{HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32}$

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

00aa00bdce0b}\inprochandler32

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

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

00aa00bdce0b}\inprochandlerx86

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

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

00aa00bdce0b}\localserver

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

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

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

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

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

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

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

00aa00686f13}\progid

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

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

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

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

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

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

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

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

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

options\mlang.dll

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

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

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

explorer\main\featurecontrol\feature_sslux

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_sslux

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

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_browser_emulation

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter

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

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

HKCU\software\classes\.css Opens kev:

Opens key: HKCR\.css

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

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

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens kev: 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

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation

HKCU\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_behaviors

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_behaviors

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

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

00aa00bdce0b}\treatas

 $HKCR \verb|\clsid|{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} \verb|\treatas|$ 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

 $HKCR \clsid \ \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\} \localserver 32$ Opens key:

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

00aa00bdce0b}\inprochandler32

 $\label{lem:hkcr} $HKCR\clsid\\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\\\nprochandler 32$ Opens key:

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

00aa00bdce0b}\inprochandlerx86

 $HKCR \c1sid \c13050f4cf-98b5-11cf-bb82-00aa00bdce0b\c1inprochandlerx86$ Opens key:

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

00aa00bdce0b}\localserver

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

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

options\iepeers.dll

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

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

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_binary_caller_service_provider

 $\label{lem:hklm} \verb+KKLM\+ software \verb+\policies+ microsoft+ internet explorer+ dxtrans \\$ Opens key:

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

Opens key: HKCU\software\classes\.js

Opens key: HKCR\.js

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_feeds

HKLM\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature feeds

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

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

settings\

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

settings\zonemap\

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

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

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

f4ceaaf59cfc}\treatas

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

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

f4ceaaf59cfc}\inprocserver32

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

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

f4ceaaf59cfc}\inprocserverx86

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

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

f4ceaaf59cfc}\localserver32

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

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

f4ceaaf59cfc}\inprochandler32

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

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

f4ceaaf59cfc}\inprochandlerx86

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

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

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: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

c9633f71be64}\languageprofile

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

c9633f71be64}\languageprofile\0x00000000

 $\label{lem:condition} Opens key: $HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-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} Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\treatas

431b3828ba53}\inprocserver32

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

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

431b3828ba53}\inprocserverx86

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

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

431b3828ba53}\localserver32

 $Opens~key: \\ HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\ \ localserver 32$

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

431b3828ba53}\inprochandler32

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32

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

431b3828ba53}\inprochandlerx86

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86

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

431b3828ba53}\localserver

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}

Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7\}
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\treatas

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 key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\localserver32

Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32

Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\inprochandler32

Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32

Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\inprochandlerx86

Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\localserver

```
HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
       Opens key:
       Opens key:
                                                                                                  HKLM\software\microsoft\ctf\tip\
                                                                                                  Opens key:
 c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
       Opens kev:
                                                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                  HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \mid c1ee01f2-b3b6-4a6a-9ddd-based \mid c1ee01f2-b3b6-4a6a-9dd-based \mid c1ee01f2-b3b6-4a6a-9dd-based \mid c1ee01f2-b3b6-4a6a-9dd-based \mid c1ee01f2-b3b6-4a6a-9dd-based \mid c1ee01f2-b3b6-4a6a-9dd-based \mid c1ee01f2-b3b6-4a6a-9db-based \mid c1ee01f2-b3b6-based \mid c1ee01f2-b3b6-based \mid c1ee01f2-b3b6-based \mid c1ee01f2-based \mid c
      Opens key:
 e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
       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
 00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                 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
       Opens kev:
0 f816 c09 f4 ee \} \\ category \\ \{b95 f181 b-ea4 c-4 af1-8056-7 c321 abb b091\} \\
       Opens key:
                                                                                                  HKCU\software\microsoft\ctf\langbaraddin\
       Opens key:
                                                                                                  HKLM\software\microsoft\ctf\langbaraddin\
       Opens key:
                                                                                                  c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
       Opens key:
 77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
      Opens key:
                                                                                                  HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
 e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
       Opens key:
                                                                                                  HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-14d}
 00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                  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 kev:
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
      Opens key:
                                                                                                  HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
 c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
       Opens key:
                                                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                                  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 key:
c9633f71be64\\ \\ \\ category\\ \\ \\ item\\ \\ \\ c6debc0a-f2b2-4f17-930e-ca9faff4cd04\\ \\ \\
                                                                                                 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\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                                                                  HKCU\software\policies\microsoft\internet explorer\control panel
       Opens kev:
                                                                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\url} \\
       Opens key:
history
       Opens key:
                                                                                                 HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_iedde_register_urlecho
       Opens key:
                                                                                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
                                                                                                 HKCU \setminus software \setminus classes \setminus clsid \setminus \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\}
       Opens key:
       Opens key:
                                                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
       Opens key:
                                                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
       Opens key:
                                                                                                  HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\treatas
                                                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
       Opens kev:
 00aa00bbbb58}\inprocserver32
                                                                                                  HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprocserver32
       Opens key:
                                                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
       Opens key:
00aa00bbbb58}\inprocserverx86
                                                                                                  HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbb58\\\inprocserverx86
       Opens key:
       Opens key:
                                                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver32
                                                                                                  HKCR \clsid \f414c260-6ac0-11cf-b6d1-00aa00bbbb58 \localserver 32
       Opens key:
       Opens key:
                                                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
       Opens key:
                                                                                                  HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprochandler32
       Opens key:
                                                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandlerx86
                                                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
       Opens key:
       Opens key:
                                                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver
       Opens key:
                                                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver
       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
                                                                                                  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}
                                                                                                  HKLM\system\currentcontrolset\control\nls\locale
       Opens key:
       Opens key:
                                                                                                  HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
       Opens key:
                                                                                                  HKLM\system\currentcontrolset\control\nls\language groups
                                                                                                  HKCU\software\classes\appid\f4cade5dce24d5c9d966cb266c7c7346.exe
       Opens key:
       Opens key:
                                                                                                  HKCR\appid\f4cade5dce24d5c9d966cb266c7c7346.exe
                                                                                                  HKLM\system\currentcontrolset\control\lsa
       Opens key:
```

HKCU\software\microsoft\internet

Opens key:

```
explorer\main\featurecontrol\feature_scripturl_mitigation
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation
                                    HKCU\software\classes\.jpg
  Opens key:
  Opens key:
                                    HKCR\.jpg
  Opens key:
                                    HKCU\software\classes\protocols\filter\image/jpeg
                                    HKCR\protocols\filter\image/jpeg
  Opens key:
  Opens key:
                                    HKCU\software\classes\.png
  Opens key:
                                    HKCR\.png
                                    HKCU\software\classes\protocols\filter\image/png
  Opens key:
  Opens key:
                                    HKCR\protocols\filter\image/png
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imgutil.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:
                                    HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
  Opens key:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
  Opens key:
                                    HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\treatas
                                    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
  Opens key:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
  Opens key:
                                    HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\localserver32
  Opens key:
                                    HKCR \c1sid \ \{30c3b080-30fb-11d0-b724-00aa006c1a01\} \localserver 32
  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\} \ in prochandler x 86 \ in proch
  Opens key:
                                    HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\localserver
  Opens key:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
                                    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:
                                    HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
                                    Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserverx86
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\label{eq:hkcr} \\
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\localserver32
                                    HKCR \clsid \end{da0-30df-11d0-b724-00aa006c1a01} \label{eq:hkcr} \\ local server 32
  Opens key:
                                    HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
  Opens kev:
00aa006c1a01}\inprochandler32
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
  Opens kev:
  Opens key:
                                    HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandlerx86
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\tinprochandlerx86
  Opens key:
  Opens key:
                                    00aa006c1a01}\localserver
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
  Opens key:
  Opens key:
                                    HKCU\software\classes\mime\database\content type
  Opens key:
                                    HKCR\mime\database\content type
  Opens key:
                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \mbox{$image/bmp\bits}$ \\
  Opens key:
                                    HKCR\mime\database\content type\image/bmp\bits
                                    HKCU\software\classes\mime\database\content type\image/gif\bits
  Opens key:
  Opens key:
                                    HKCR\mime\database\content type\image/gif\bits
  Opens key:
                                    HKCU\software\classes\mime\database\content type\image/jpeg\bits
  Opens key:
                                    HKCR\mime\database\content type\image/jpeg\bits
  Opens key:
                                    HKCU\software\classes\mime\database\content type\image/pjpeg\bits
  Opens key:
                                    HKCR\mime\database\content type\image/pjpeg\bits
  Opens kev:
                                    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
                                    HKCU\software\classes\mime\database\content type\image/x-icon\bits
  Opens key:
  Opens key:
                                    HKCR\mime\database\content type\image/x-icon\bits
```

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

HKCR\mime\database\content type\image/x-jg\bits

Opens kev:

Opens key:

Opens key: HKCU\software\classes\mime\database\content type\image/x-png\bits Opens key: HKCR\mime\database\content type\image/x-png\bits Opens kev: HKCU\software\classes\mime\database\content type\image/x-wmf\bits HKCR\mime\database\content type\image/x-wmf\bits Opens key: Opens key: HKCU\software\classes\mime\database\content type\image/x-png Opens key: HKCR\mime\database\content type\image/x-png $HKCU \setminus software \setminus classes \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-00a0c913f750\}$ Opens key: Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750} Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas Opens kev: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86 Opens key: Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32 Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32 Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32 Opens kev: Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86 Opens key: Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\pngfilt.dll 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 HKLM\software\microsoft\internet explorer\services Opens key: Opens key: HKLM\software\policies\microsoft\internet explorer\activities Opens key: HKCU\software\microsoft\internet explorer\activities HKLM\software\microsoft\internet explorer\activities Opens key: Opens key: HKLM\software\policies\microsoft\internet explorer\infodelivery\restrictions HKCU\software\policies\microsoft\internet Opens key: explorer\infodelivery\restrictions Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites HKCU\software\microsoft\internet explorer\suggested sites Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\xml.dll $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet\ explorer\+ feed\ discovery$ Opens key: Opens key: HKLM\software\microsoft\internet explorer\feed discovery Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_isolate_named_windows HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature isolate named windows Opens key: HKCU\software\classes\protocols\name-space handler\http\ Opens key: HKCR\protocols\name-space handler\http HKCU\software\microsoft\windows\currentversion\internet settings\user Opens key: agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent Opens kev: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent Opens key: $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} user \end{tabular}$ agent\ua tokens Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} user \end{tabular}$ agent\pre platform Opens kev: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\5.0\user agent\pre platform Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\post platform Opens kev: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ 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 kev: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_maxconnectionsper1_0server

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

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

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

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

fd2b31b3eefd}\treatas

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

fd2b31b3eefd}\inprocserver32

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

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

fd2b31b3eefd}\inprocserverx86

Opens key: $HKCR\clsid\\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\\{inprocserverx86}$

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

fd2b31b3eefd}\localserver32

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

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

fd2b31b3eefd}\inprochandler32

 $HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\nprochandler32$ Opens key:

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

fd2b31b3eefd}\inprochandlerx86

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

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

fd2b31b3eefd}\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

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

options\nsarray.dll

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

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

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

Opens key: HKCU\appevents\schemes\apps\explorer\activatingdocument\.current

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert

HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ fileexts$ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm

Opens key: HKCU\software\classes\htmlfile

HKCR\htmlfile Opens key:

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

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

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

Opens key: HKCR\htmlfile\shellex\iconhandler HKCU\software\classes\systemfileassociations\.htm Opens key:

Opens key: HKCR\systemfileassociations\.htm

Opens key:

HKCU\software\classes\systemfileassociations\text

HKCR\systemfileassociations\text Opens key: Opens key: HKCU\software\classes\htmlfile\clsid

Opens key: HKCR\htmlfile\clsid

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

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

13914bef5890}

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

Opens key: $HKCU \setminus software \setminus classes \setminus system file associations \setminus text \setminus shellex \setminus \{a39ee748-text\} = \{a39ee748-$

6a27-4817-a6f2-13914bef5890}

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

13914bef5890}

HKCU\software\classes* Opens kev:

Opens key: HKCR*

```
Opens key:
                    HKCU\software\classes\*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
 Opens key:
                    HKCR\*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
                    Opens key:
000000000046}
 Opens key:
                    HKCR\htmlfile\shellex\{000214e6-0000-0000-c000-00000000046}
```

Opens key:

000000000046}

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

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

0000-0000-c000-000000000046}

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

000000000046}

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

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

explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_crossdomain_fix_kb867801 Opens kev: 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: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \the memanager \end{tabular}$ 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}\inprochandler32 Opens key:

Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-

00aa003f8646}\inprochandlerx86

HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-

00aa003f8646}\localserver

HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\}$

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}

 $HKCU \setminus software \\ classes \\ \clsid \\ \{ff393560-c2a7-11cf-bff4-444553540000\} \\ \clsid \\ \cls$ Opens key:

Opens key: $\label{local-equation-of-bff4-444553540000} \verb|\delta| ff393560-c2a7-11cf-bff4-444553540000 \verb|\delta| shell | ff39360-c2a7-11cf-bff4-444553540000 \verb|\delta| shell | ff39360-c2a$ HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens kev:

444553540000}\shellex\iconhandler

 $\label{lem:hkcr} \begin{tabular}{ll} HKCR\clsid\ff393560-c2a7-11cf-bff4-444553540000}\shellex\clsid\ff393560-c2a7-11cf-bff4-444553540000\end{tabular} \label{lem:hkcr}$ Opens key: $HKCU \setminus software \\ \\ classes \\ \\ clsid \\ \\ ff393560-c2a7-11cf-bff4-444553540000 \\ \\ \\ \\ clsid$ Opens key:

HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid Opens kev: Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprocserver32

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\treatas

HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens kev:

444553540000}\inprocserverx86

Opens key:

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\localserver32

HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32 Opens key:

HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens kev:

444553540000}\inprochandler32

Opens key:

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprochandlerx86

HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandlerx86 Opens key:

HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens key:

444553540000}\localserver

HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver Opens key:

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ lobjects \ \{ff 393560-c2a7-11cf-market \ microsoft \ mic$ bff4-444553540000}

```
HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\5.0\cache\extensible cache\mshist012016042820160429
    Opens key:
                                                      HKCU\software\microsoft\internet explorer\main\windowssearch
                                                      HKLM\software\policies\microsoft\internet explorer\feeds
    Opens key:
    Opens key:
                                                      HKCU\software\microsoft\internet explorer\feeds
    Opens key:
                                                      HKLM\software\microsoft\internet explorer\feeds
    Opens key:
                                                      HKCU\software\classes\.url\persistenthandler
                                                      HKCR\.url\persistenthandler
    Opens key:
    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 kev:
08002b30309d}\shellfolder
    Opens key:
                                                      HKCU \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus (20d04feo-block) + 
    Opens key:
3aea-1069-a2d8-08002b30309d}
    Opens key:
                                                      HKCU\software\microsoft\windows\currentversion\policies\nonenum
                                                      HKI M\software\microsoft\windows\currentversion\policies\nonenum
    Opens kev:
    Opens key:
                                                      HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus 
3aea-1069-a2d8-08002b30309d}\shellfolder
                                                      Opens key:
3aea-1069-a2d8-08002b30309d}\shellfolder
    Opens key:
                                                      HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
                                                      HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
    Opens kev:
    Opens key:
                                                      HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\
    Opens key:
                                                      HKCU\software\microsoft\windows\shellnoroam
    Opens key:
                                                      HKCU\software\microsoft\windows\shellnoroam\muicache
    Opens key:
                                                      HKCU\software\microsoft\windows\shellnoroam\muicache\
    Opens key:
                                                      HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
    Opens key:
                                                      HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                      Opens key:
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
    Opens key:
                                                      HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1\} \\ category \\ item \\ \{a48fa74e-f767-44e4-bfbc-169e8b38ff58\} \\
                                                      HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
Of816c09f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
    Queries value:
                                                      HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Queries value:
                                                      HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
                                                      HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value:
                                                     HKLM\software\microsoft\windows
nt\currentversion\compatibility32[f4cade5dce24d5c9d966cb266c7c7346]
                                                     HKLM\software\microsoft\windows nt\currentversion\ime
    Queries value:
compatibility[f4cade5dce24d5c9d966cb266c7c7346]
    Queries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
    Oueries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
    Queries value:
                                                      HKLM\system\setup[systemsetupinprogress]
                                                      HKCU\control panel\desktop[multiuilanguageid]
    Oueries value:
                                                      HKCU\control panel\desktop[smoothscroll]
    Oueries value:
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
                                                      HKLM\system\currentcontrolset\control\session
    Oueries value:
manager[criticalsectiontimeout]
                                                      HKLM\software\microsoft\ole[rwlockresourcetimeout]
    Queries value:
                                                      HKCR\interface[interfacehelperdisableall]
    Oueries value:
    Oueries value:
                                                      HKCR\interface[interfacehelperdisableallforole32]
                                                      HKCR\interface[interfacehelperdisabletypelib]
    Queries value:
    Queries value:
                                                      HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
                                                      HKCR\interface\{00020400-0000-0000-c000-
    Queries value:
00000000046}[interfacehelperdisableallforole32]
                                                      HKLM\software\microsoft\ctf\systemshared[cuas]
    Oueries value:
                                                      HKCU\keyboard layout\toggle[language hotkey]
    Oueries value:
    Queries value:
                                                      HKCU\keyboard layout\toggle[hotkey]
    Oueries value:
                                                      HKCU\keyboard layout\toggle[layout hotkey]
    Queries value:
                                                      HKLM\software\microsoft\ctf[enableanchorcontext]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
                                                      HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
    Oueries value:
```

HKLM\system\wpa\pnp[seed]

Queries value:

Oueries value: HKLM\system\setup[osloaderpath] HKLM\system\setup[systempartition] Oueries value:

Oueries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Queries value:

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

Queries value:

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

HKLM\software\microsoft\windows\currentversion\setup[drivercachepath] Oueries value:

Oueries value: HKLM\software\microsoft\windows\currentversion[devicepath] Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]

Queries value:

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

 $HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[| hostname]|$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]

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

Oueries value:

11e3-9fc7-806d6172696f}[data]

Queries value:

11e3-9fc7-806d6172696f}[generation]

HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Oueries value:

409d6c4515e9}[drivemask]

Queries value:

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]

Queries value:

 $\label{thm:local_explorer} \begin{tabular}{l} HKCU \software \mbox{$\mbox{$m$icrosoft}$ windows \current version \policies \explorer [nowebview] \end{tabular}$

Queries value:

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

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

Queries value:

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

Queries value:

 $HKCU \ software \ microsoft \ windows \ current version \ policies \ explorer \ [no simple startmenu]$

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

Oueries value:

 $HKCU \ software \ \verb|microsoft| windows \ \verb|currentversion| explorer \ | advanced [showcompcolor] | the software \ | advanced \ | adva$

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

Queries value:

Oueries value:

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

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

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

Oueries value:

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

Oueries value:

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

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

Oueries value:

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

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

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

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

settings[disableimprovedzonecheck]

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature protocol lockdown[f4cade5dce24d5c9d966cb266c7c7346.exel

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

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

ab78-1084642581fb]

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

0000-00000000000001

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

manager[safeprocesssearchmode]

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

manager\appcompatibility[disableappcompat]

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

Oueries value:

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

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

be2efd2c1a33}[itemdata]

Oueries value:

be2efd2c1a33}[saferflags]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

b813f72dbb91}[hashalg]

Oueries value:

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

Queries value:

b813f72dbb91}[saferflags]

Oueries value:

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

Queries value:

7c29ddecae3f}[hashalg]

Queries value:

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

Queries value:

7c29ddecae3f}[saferflags]

Queries value:

085bcc18a68d}[itemdata]

Queries value:

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

Queries value:

085bcc18a68d}[itemsize]

Queries value:

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

Oueries value:

b91490411bfc}[itemdata]

Queries value:

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

Queries value:

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

Queries value:

b91490411bfc}[saferflags]

Queries value:

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

Oueries value:

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

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

folders[cache]

Queries value:

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

HKLM\software\microsoft\windows nt\currentversion\compatibilitv32[bil Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[bi]

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[fromcachetimeout]

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[secureprotocols]
                           HKLM\software\policies\microsoft\internet
 Oueries value:
explorer\main[security_hklm_only]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
 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[disablekeepalive]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablepassport]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablebasicoverclearchannel]
                           HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                           HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[syncmode5]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
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
 Queries value:
settings\5.0\cache\content[peruseritem]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[cache]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\cookies[peruseritem]
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \user shell \end{tabular}
 Queries value:
folders[cookies]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[cachelimit]
 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\historv[peruseritem]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[history]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                           HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_protocol_lockdown[bi.exe]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
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
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
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]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[maxconnectionsper1_0server]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 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[maxconnectionsperproxy]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Queries value:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[connecttimeout]
 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[connectretries]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 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[disablentlmpreauth]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                           HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
 Queries value:
                           HKCU\software\microsoft\ctf[disable thread input manager]
 Queries value:
 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[f4cade5dce24d5c9d966cb266c7c7346.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]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[perusercookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablent4rascheck]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendextracrlf]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bvpassftptimecheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Queries value:
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[releasesocketduring401auth]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablelegacypreauthasserver]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Oueries 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
 Oueries value:
settings[mimeexclusionlistforcache]
```

```
Oueries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnalwaysonpost]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonzonecrossing]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonbadcertsending]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertrecving]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpostredirect]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[alwaysdrainonredirect]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonhttpstohttpredirect]
 Queries 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:
Queries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 0000000000005 \ [packed catalog item]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 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]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace \_catalog5 \ catalog\_entries \ 00000000001 [library path]
 Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 000000000001[providerid]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 00000000001 \ [address family]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
```

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000002 [address family])$

Queries value:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002[supported name space]]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ namespace\_catalog \ namespace\_
   Queries 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\00000000003[librarypath]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 \setminus catalog\_entries \setminus 000000000003 [displaystring]
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000003 [supported name space]]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000003[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[globaluseroffline]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enableautodial]
                                                   HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[urlencoding]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[truncatefilename]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[badproxvexpirestime]
                                                  HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[bi.exe]
                                                  HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_mime_handling[bi.exe]
                                                   HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature mime handling[*]
   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 \setminus software \setminus microsoft \setminus internet explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus microsoft \setminus microso
472f-a0ff-e1416b8b2e3a}[url]
   Queries value:
                                                   HKLM\system\currentcontrolset\control\session
manager\environment[processor_architecture]
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Oueries value:
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Oueries value:
                                                   HKLM\software\microsoft\net framework setup\ndp\v2.0.50727[install]
                                                   HKLM\software\microsoft\net\ framework\ setup\ndp\v2.0.50727[sp]
   Oueries value:
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
   Oueries value:
                                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 8]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midil
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
   Oueries value:
                                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi4]
   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\net framework setup\ndp\v3.5[install]
                                                   HKLM\software\microsoft\net framework setup\ndp\v3.5[sp]
   Oueries value:
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi51]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi81]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
   Oueries 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]
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]

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

Queries value:

Oueries value:

Queries value:

```
Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion[currentversion]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
 Oueries value:
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
 Oueries 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]
 Oueries 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]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32\mixer81
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
 Queries value:
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
                          HKLM\software\microsoft\tracing[enableconsoletracing]
 Oueries value:
 Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
 Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
                           HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
 Oueries value:
 Queries value:
                           HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [consoletracing mask]
 Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
 Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[filedirectory]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[userenvdebuglevel]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
                           HKLM\system\currentcontrolset\control\productoptions[producttype]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[personal]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[local settings]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\winlogon[rsopdebuglevel]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\profilelist[allusersprofile]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
                          HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion[commonfilesdir]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 Oueries value:
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]
                          HKLM\software\microsoft\com3[com+enabled]
 Oueries value:
                          HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
 Oueries value:
                           {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create object]}
 Queries value:
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[f4cade5dce24d5c9d966cb266c7c7346.exe]
                          HKLM\software\microsoft\com3[regdbversion]
 Queries value:
                          HKCR\clsid\{8856f961-340a-11d0-a96b-
 Oueries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
 Oueries value:
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\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:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\connections[savedlegacysettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\connections[defaultconnectionsettings]
 Queries value:
                          HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
                          HKCR\clsid\{8856f961-340a-11d0-a96b-
 Oueries value:
```

00c04fd705a2}\inprocserver32[threadingmodel]

```
Oueries value:
                                                HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
                                                HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
   Oueries value:
   Oueries value:
                                                HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
   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]
                                               HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
   Oueries value:
   Oueries value:
                                               HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
                                                HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
   Queries value:
                                               HKCR \land extraction{HKCR \ ext
   Oueries value:
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:
\label{lem:hklm} \verb+KLM\+ system \verb+ current control set \verb+ services \verb+ tcpip \verb+ parameters [allow unqualified query]+ of the property of the 
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:
                                               HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
   Queries value:
                                               HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[createuricachesize]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
                                               HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[createuricachesize]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]
```

```
Oueries value:
                                  HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
                                  HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
  Oueries value:
  Oueries value:
                                  HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [maxnegative cachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
                                 HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
  Oueries value:
c7d49d7cecdc}[enabledhcp]
  Queries value:
c7d49d7cecdc}[leaseobtainedtime]
  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}[leaseterminatestime]
  Queries value:
c7d49d7cecdc}[dhcpserver]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablepunycode]
                                 HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablepunycode]
                                  HKLM\software\microsoft\internet explorer\main[navigationdelay]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:
  Oueries value:
                                  HKLM\software\microsoft\internet explorer\main[frametabwindow]
                                  HKCU\software\microsoft\internet explorer\main[framemerging]
  Queries value:
                                  HKLM\software\microsoft\internet explorer\main[framemerging]
  Oueries value:
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[sessionmerging]
                                  HKLM\software\microsoft\internet explorer\main[sessionmerging]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:
  Queries value:
                                  HKLM\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:
                                  HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
                                  HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
  Queries value:
                                  HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
                                  HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
  Oueries value:
                                  HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[loadwithoutcom]
                                 HKLM\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Queries value:
                                 HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Oueries value:
                                 HKLM\software\microsoft\rpc\securityservice[10]
  Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
                                  HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0x4011
                                  \label{local-objective} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\shell}} \\
0x4011
  Oueries value:
HKLM\svstem\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
  Queries value:
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
  Queries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\msapsspc.dll[version]
  Queries value:
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
  Oueries value:
Oueries value:
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
  Queries value:
```

c7d49d7cecdc}[queryadaptername]

Oueries value: c7d49d7cecdc}[disableadapterdomainname] c7d49d7cecdc}[registrationenabled] Oueries value: c7d49d7cecdc}[registeradaptername] c7d49d7cecdc}[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[maxnumberofaddressestoregister] 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] HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment] Queries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize] Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[inprocserver32] Queries value: c7d49d7cecdc}[ipautoconfigurationenabled] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[addresstype] 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}[nameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Oueries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder] HKCR\clsid\{871c5380-42a0-1069-a2ea-Oueries value: 08002b30309d}\inprocserver32[threadingmodel] HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Oueries value: cryptographic provider[type] Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu] Oueries value: HKCR\protocols\handler\res[clsid] Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32] HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[] Oueries value: Queries value: $HKCR \clsid \ \{3050f3bc-98b5-11cf-bb82-00aa00bdce0b\} [appid]$ Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel] HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[f4cade5dce24d5c9d966cb266c7c7346.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[*] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching[f4cade5dce24d5c9d966cb266c7c7346.exe] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_object_caching[*] Oueries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]

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

HKLM\software\microsoft\internet explorer\application

Queries value:

compatibility[f4cade5dce24d5c9d966cb266c7c7346.exe]

Oueries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit] HKLM\software\microsoft\windows\currentversion\policies\ratings[key] Oueries value:

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

settings[urlencoding]

HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]

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

explorer\security[disablesecuritysettingscheck]

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

settings\zones\0[flags]

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

settings\zones\1[flags]

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

settings\zones\2[flags]

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

settings\zones\3[flags]

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

settings\zones\4[flags]

HKCU\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_localmachine_lockdown[f4cade5dce24d5c9d966cb266c7c7346.exe]

Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*] Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_localmachine_lockdown[f4cade5dce24d5c9d966cb266c7c7346.exe]

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

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

Oueries value:

settings[specialfolderscachesize]

HKCU\software\microsoft\internet explorer[no3dborder] Oueries value: HKLM\software\microsoft\internet explorer[no3dborder] Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize] Queries value:

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

explorer\main\featurecontrol\feature_mime_sniffing[f4cade5dce24d5c9d966cb266c7c7346.exe]

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

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

settings[istextplainhonored]

HKLM\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_safe_bindtoobject[f4cade5dce24d5c9d966cb266c7c7346.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[] Queries value:

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

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

00aa00686f13}\inprocserver32[threadingmodel]

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

HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [helperdllname]$

HKCU\software\microsoft\windows Queries value: nt\currentversion\windows[dragscrollinset]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrolldelay]

HKCU\software\microsoft\windows Queries value:

nt\currentversion\windows[dragscrollinterval]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_restrict_filedownload[f4cade5dce24d5c9d966cb266c7c7346.exe]

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

00aa00bdce0b}\inprocserver32[inprocserver32]

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

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

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

00aa00bdce0b}\inprocserver32[threadingmodel]

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

settings\zones\3[2106]

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

settings\zones\3[2106]

Oueries value: HKCU\software\microsoft\internet explorer\zoom[zoomdisabled] HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[] Oueries value: Oueries value: HKLM\software\policies\microsoft\internet explorer[smartdithering] HKCU\software\microsoft\internet explorer[smartdithering] Queries value: Oueries value: 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 explorer\main[page_transitions] Queries value: HKCU\software\microsoft\internet explorer\main[page_transitions] HKLM\software\policies\microsoft\internet Oueries value: explorer\main[use_dlgbox_colors] Queries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] Queries value: HKLM\software\policies\microsoft\internet explorer\main[anchor underline] Queries value: HKCU\software\microsoft\internet explorer\main[anchor underline] HKCU\software\microsoft\internet explorer\main[css_compat] Oueries value: Queries 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] Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline videos1 Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos] Queries value: HKLM\software\policies\microsoft\internet explorer\main[play_background_sounds] Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\internet} explorer\mbox{\tt main[play_background_sounds]}}$ Queries value: HKLM\software\policies\microsoft\internet explorer\main[play_animations] Oueries value: HKCU\software\microsoft\internet explorer\main[play_animations] Queries value: HKLM\software\policies\microsoft\internet explorer\main[print_background] HKCU\software\microsoft\internet explorer\main[print_background] Queries value: Queries value: HKCU\software\microsoft\internet explorer\main[use stylesheets] Queries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll] Oueries value: HKCU\software\microsoft\internet explorer\main[smoothscroll] HKLM\software\policies\microsoft\internet explorer\main[xmlhttp] Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp] Oueries value: Oueries value: HKLM\software\policies\microsoft\internet explorer\main[show image placeholders] HKCU\software\microsoft\internet explorer\main[show image placeholders] Queries value: Queries value: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ internet\ explorer\+ main[disable\ script\]$ debugger] Queries value: HKCU\software\microsoft\internet explorer\main[disable script debugger] HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie] Queries value: HKCU\software\microsoft\internet explorer\main[move system caret] Oueries value: HKCU\software\microsoft\internet explorer\main[force offscreen Queries value: composition] Queries value: HKLM\software\policies\microsoft\internet explorer\main[enable autoimageresizel Queries value: HKCU\software\microsoft\internet explorer\main[enable autoimageresize] HKCU\software\microsoft\internet explorer\main[usethemes] Oueries value: HKCU\software\microsoft\internet explorer\main[usehr] Oueries value: Oueries value: HKCU\software\microsoft\internet explorer\main[q300829] HKCU\software\microsoft\internet explorer\main[cleanup htcs] Queries value: Oueries value: HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]

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

Queries value: HKCU\software\microsoft\internet

explorer\international[default_codepage]

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

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

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

size]

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

face]

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

hyperlinks]

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

color]

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

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

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefontsize]

HKCU\software\microsoft\internet Queries value: explorer\international\scripts\3[iefontsizeprivate] Oueries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iepropfontname] Oueries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefixedfontname] HKCU\software\microsoft\internet explorer\international[acceptlanguage] Oueries value: HKLM\software\microsoft\internet explorer\version vector[vml] Oueries value: Oueries value: HKLM\software\microsoft\internet explorer\version vector[ie] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[f4cade5dce24d5c9d966cb266c7c7346.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[*] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2700] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[2700] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[f4cade5dce24d5c9d966cb266c7c7346.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_xssfilter[*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones[securitysafe] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nofileurl] $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ 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] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[cointernetcombineiuricachesize] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown[f4cade5dce24d5c9d966cb266c7c7346.exe] HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown[*] Oueries value: HKCR\.css[content type] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_behaviors[f4cade5dce24d5c9d966cb266c7c7346.exe] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors[*] HKCU\software\microsoft\windows\currentversion\internet Oueries value: 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] Queries value: $HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]$ HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid] Oueries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-Queries value: 00aa00bdce0b}\inprocserver32[threadingmodel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\0[1400] Queries value: HKCR\.js[content type] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_feeds[f4cade5dce24d5c9d966cb266c7c7346.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_feeds[*] Oueries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations2] Queries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnonintranet] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[warnonintranet] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect] Queries value: HKCR\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprocserver32[inprocserver32] HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[] Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid] Oueries value: Oueries value: HKCR\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprocserver32[threadingmodel] Queries value: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8 $c9633f71be64\\ \label{lem:c9633f71be64} \\ \labe$

Queries value: HKLM\Software\microsoft\CtT\tip\{1188450c-Tdab-4/ae-80d8c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83431b3828ba53}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\[appid]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\[appid]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\[appid]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\[appid]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-

```
869523e2d6c7}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
  Queries value:
                                    HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
  Oueries value:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
  Oueries value:
77e8f3d1aa80\} \land (c6debc0a-f2b2-4f17-930e-ca9faff4cd04) [description]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
  Oueries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1201]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                    HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
  Queries value:
                                    HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
                                    HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:
                                    HKCR\.jpg[content type]
  Queries value:
                                    HKCR\.png[content type]
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-
  Queries value:
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-
  Queries value:
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
                                    \label{local-condition} HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\ \ inprocserver32[]
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-
  Oueries value:
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries 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]
  Queries value:
                                    HKCR\mime\database\content type\image/pjpeg\bits[0]
                                    HKCR\mime\database\content type\image/png\bits[0]
  Oueries value:
                                    HKCR\mime\database\content type\image/x-png\bits[0]
  Oueries value:
  Queries value:
                                    HKCR\mime\database\content type\image/x-wmf\bits[0]
                                    HKCR\mime\database\content type\image/x-png[image filter clsid]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Queries value:
  Queries value:
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
  Queries value:
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
                                    HKCU\software\microsoft\internet explorer\recovery[autorecover]
  Queries value:
  Oueries value:
                                    HKCU\software\microsoft\ftp[use web based ftp]
  Queries value:
                                    HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
                                    HKCU\software\microsoft\internet explorer\suggested sites[enabled]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[local appdata]
  Queries value:
                                    HKLM\software\microsoft\internet explorer\feed discovery[sound]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2700]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\3[2700]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[compatible]
                                    \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
  Oueries value:
settings\5.0\user agent[compatible]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[platform]
```

```
Queries value:
                                     HKLM\software\microsoft\internet
explorer \verb|\main\featurecontrol\feature\_| maxconnection sperserver [f4cade5dce24d5c9d966cb266c7c7346.exe]|
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver[f4cade5dce24d5c9d966cb266c7c7346.exe]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
  Queries value:
                                    HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
  Oueries value:
  Queries value:
                                     HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}[appid]
  Queries value:
                                    HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[1a10]
                                    HKCU\software\microsoft\internet explorer\main[autosearch]
  Oueries value:
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[friendly http errors]
  Oueries value:
                                     HKLM\software\microsoft\internet explorer[version]
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion[productname]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion[productname]
  Queries value:
                                     HKLM\system\currentcontrolset\control\windows[csdversion]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\3[currentlevel]
  Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [allow filecl sidjunctions]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[progid]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[application]
  Queries value:
                                    HKCR\.htm[]
                                    HKCR\htmlfile\shellex\iconhandler[]
  Queries value:
  Queries value:
                                     HKCR\htmlfile[docobject]
  Queries value:
                                     HKCR\.htm[perceivedtype]
  Oueries value:
                                     HKCR\systemfileassociations\text[docobject]
  Queries value:
                                     HKCR\htmlfile[browseinplace]
  Queries value:
                                     HKCR\systemfileassociations\text[browseinplace]
                                     HKCR\htmlfile\clsid[]
  Oueries value:
  Queries value:
                                     HKCR\htmlfile[isshortcut]
                                     HKCR\systemfileassociations\text[isshortcut]
  Queries value:
                                     HKCR\htmlfile[alwaysshowext]
  Oueries value:
  Queries value:
                                     HKCR\systemfileassociations\text[alwaysshowext]
  Queries value:
                                     HKCR\htmlfile[nevershowext]
                                     {\tt HKCR} \verb|\systemfileassociations \verb|\text[nevershowext]|
  Oueries value:
                                     HKCU\appevents\schemes\apps\explorer\navigating\.current[]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[recent]
  Queries value:
                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| the memanager [compositing] \end{tabular}
                                     HKCU\control panel\desktop[lamebuttontext]
  Oueries value:
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Queries value:
00aa003f8646}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[appid]
  Oueries value:
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Queries value:
00aa003f8646}\inprocserver32[threadingmodel]
                                    HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1256]
                                     HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Queries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[874]
                                     HKLM\system\currentcontrolset\control\nls\codepage[932]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[949]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
  Oueries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobject]
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}[browseinplace]
  Oueries value:
  Queries value:
                                     \label{local-equation-of-bff4-444553540000} HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\[isshortcut]
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[alwaysshowext]
  Oueries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}[nevershowext]
  Queries value:
                                     \label{lem:hkcr} $$ HKCR\clsid{ff393560-c2a7-11cf-bff4-444553540000} \in \clsid{ff393560-c2a7-11cf-bff4-444553540000} in processing the second context of 
  Oueries value:
  Oueries value:
                                    HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[loadwithoutcom]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\shell
```

```
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
                                                                                      HKLM\software\microsoft\windows\currentversion\shell
      Oueries value:
extensions \\ cached \cite{ff393560-c2a7-11cf-bff4-444553540000} \\ \cite{eq2b1e2-a19e-4b43-8160-7bcecacb3d6e} 
0x4011
      Oueries value:
                                                                                       HKCU\software\microsoft\windows\currentversion\shell
 extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x4011
                                                                                      HKCR\clsid\{ff393560-c2a7-11cf-bff4-
      Oueries value:
444553540000}\inprocserver32[inprocserver32]
                                                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
      Oueries value:
                                                                                      HKCR\clsid\{ff393560-c2a7-11cf-bff4-
      Oueries value:
444553540000}\inprocserver32[threadingmodel]
      Queries value:
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair]
      Queries value:
                                                                                       HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
      Oueries value:
 settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix]
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
     Queries 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]
                                                                                      HKCU\software\microsoft\internet
      Oueries value:
 explorer\main\windowssearch[enabledscopes]
                                                                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
      Queries value:
 folders[favorites]
      Queries value:
                                                                                       HKCR\.url\persistenthandler[]
      Queries value:
                                                                                       HKLM\software\microsoft\windows search[currentversion]
                                                                                      HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
      Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                                                                      HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value:
 08002b30309d}\shellfolder[attributes]
                                                                                       HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
      Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}1
                                                                                       HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
      Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                                                                       HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
      Queries value:
      Oueries value:
                                                                                      HKLM \  \  \, nt\  \  \, \
 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]
      Queries value:
                                                                                      HKLM \  \  \, nt\  \  \, \
 1757981266-507921405-1957994488-1003[centralprofile]
     Oueries value:
                                                                                      HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 1757981266-507921405-1957994488-1003[profileloadtimelow]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 1757981266-507921405-1957994488-1003[profileloadtimehigh]
      Queries value:
                                                                                      HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
      Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll.-92161
      Queries value:
                                                                                       HKLM\software\microsoft\internet explorer\main[maxrenderline]
                                                                                       HKCU\software\appdatalow\software\smartbar[globaluserid]
      Sets/Creates value:
     Sets/Creates value:
                                                                                       HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
                                                                                       HKCU\software\conduit\distributionengine\1\offerhistory\755131[offerid]
      Sets/Creates value:
      Sets/Creates value:
                                                                                       HKCU\software\conduit\distributionengine\1\offerhistory\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:
                                                                                       HKCU\software\conduit\distributionengine\1\offerhistory\755131[ruleid]
      Sets/Creates value:
HKCU \setminus software \setminus conduit \setminus distribution engine \setminus 1 \setminus offerhistory \setminus 755131 [root offerid]
                                                                                       HKCU\software\microsoft\windows\currentversion\internet
     Sets/Creates value:
 settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
     Sets/Creates value:
                                                                                       \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma of the 
 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]
     Sets/Creates value:
                                                                                       HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions]
     Sets/Creates value:
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair]
      Value changes:
                                                                                      HKLM\software\microsoft\cryptography\rng[seed]
      Value changes:
806d6172696f}[baseclass]
```

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

folders[cache]

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

folders[cookies]

 $\label{thm:condition} Value\ changes: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ shell$

folders[history]

 $\label{thm:local_continuous} Value\ changes: \\ HKLM\ software\ microsoft\ windows\ current version\ (explorer\ shell). \\$

folders[common appdata]

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

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

 $\label{thm:condition} Value\ changes: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ shell$

folders[local appdata]

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

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

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

folders[favorites]

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

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

manager[pendingfilerenameoperations]