Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3317, Task ID: 776

Task ID:	776
Risk Level:	10
Date Processed:	2016-05-18 10:37:05 (UTC)
Processing Time:	61.58 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\57f19466903ed1ef8c74ef4d8c044ddf.exe"
Sample ID:	3317
Type:	basic
Owner:	admin
Label:	57f19466903ed1ef8c74ef4d8c044ddf
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	123930 bytes
MD5:	57f19466903ed1ef8c74ef4d8c044ddf
SHA256:	4dff3c207a81610c4c3a9294dae7bb15471ab1694aff5104bf0d9ded5e6e3264
Description:	None

Pattern Matching Results

6	Writes to system32 folder
2	PE: Nonstandard section
10	Creates malicious events: Allaple [Worm]
1	SSL traffic on standard port
4	Terminates process under Windows subfolder
5	Creates process in suspicious location
5	PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\57f19466903ed1ef8c74ef4d8c044ddf.exe ["c:\windows\temp\57f19466903ed1ef8c74ef4d8c044ddf.exe"]
Creates process:	C:\WINDOWS\system32\urdvxc.exe [C:\WINDOWS\system32\urdvxc.exe /installservice]
Creates process:	C:\WINDOWS\system32\urdvxc.exe [C:\WINDOWS\system32\urdvxc.exe /start]
Creates process:	C:\WINDOWS\system32\urdvxc.exe [C:\WINDOWS\system32\urdvxc.exe /uninstallservice patch:c:\windows\temp\57f19466903ed1ef8c74ef4d8c044ddf.exe]
Creates process:	C:\WINDOWS\system32\urdvxc.exe ["C:\WINDOWS\system32\urdvxc.exe" /service]
Terminates process:	C:\WINDOWS\Temp\57f19466903ed1ef8c74ef4d8c044ddf.exe
Terminates process:	C:\WINDOWS\system32\urdvxc.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\jhdheddfffffhjk5trh
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\WINDOWS\system32\urdvxc.exe
Opens:	C:\WINDOWS\Prefetch\57F19466903ED1EF8C74EF4D8C044-23ABD3B7.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\Temp\57f19466903ed1ef8c74ef4d8c044ddf.exe
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\shell32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\shell32.dll.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Config
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\icmp.dll
Opens:	C:\WINDOWS\system32\iphlpapi.dll
Opens:	C:\WINDOWS\system32
Opens:	C:\WINDOWS\system32\urdvxc.exe
Opens:	C:\WINDOWS\system32\apphelp.dll
Opens:	C:\WINDOWS\AppPatch\sysmain.sdb

```
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\
  Opens:                  C:\WINDOWS
  Opens:                  C:\WINDOWS\system32\urdvxc.exe.Manifest
  Opens:                  C:\WINDOWS\Prefetch\URDVXC.EXE-079A7CB0.pf
  Opens:                  C:\WINDOWS\Temp\4a6862a7-73d1-4c69-878e-d300dde95fd1
  Opens:                  C:\WINDOWS\system32\rsaenh.dll
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\Documents and Settings
  Opens:                  C:\Documents and Settings\Admin\Application Data
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\Forms
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache\7PLTA3CP
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\all
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\brt
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\can
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\eng
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\LogTransport2
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\LogTransport2\Logs
  Opens:                  C:\Documents and Settings\Admin\Application Data\Identities
  Opens:                  C:\Documents and Settings\Admin\Application Data\Identities\{5792731B-
1E8B-4ECF-8560-0E560368800D}
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer
  Opens:                  C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\AddIns
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Credentials
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Media Player
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\MMC
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Office
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Office\Recent
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Speech
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Speech\Files
  Opens:                  C:\Documents and Settings\Admin\Application
```

```
Data\Microsoft\Speech\Files\UserLexicons
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\Certificates
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CRLs
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CTLs
  Opens:                 C:\Documents and Settings\Admin\Application Data\Microsoft\Templates
  Opens:                 C:\Documents and Settings\Admin\Application Data\Microsoft\Windows
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes
  Opens:                 C:\Documents and Settings\Admin\Application Data\Oracle
  Opens:                 C:\Documents and Settings\Admin\Application Data\Oracle\Java
  Opens:                 C:\Documents and Settings\Admin\Application Data\Oracle\Java\Uninstall
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun\Java
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun\Java\AU
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\0
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\1
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\10
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\11
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\13
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\14
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\15
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\16
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\18
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\2
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\20
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\21
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\22
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\23
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\24
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\25
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\26
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\27
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\28
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\29
  Opens:                 C:\WINDOWS\system32\mswsock.dll
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\3
  Opens:                 C:\WINDOWS\system32\hnetcfg.dll
  Opens:                 C:\WINDOWS\system32\wshtcpip.dll
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\30
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\31
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\32
```

```
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\33
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\34
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\35
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\36
  Opens:                    C:\WINDOWS\system32\dnsapi.dll
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\37
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\38
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\39
  Opens:                    C:\WINDOWS\system32\winrnr.dll
  Opens:                    C:\WINDOWS\system32\drivers\etc\hosts
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\4
  Opens:                    C:\WINDOWS\system32\rasadhlp.dll
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\40
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\41
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\42
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\44
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\45
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\46
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\47
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\48
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\49
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\5
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\50
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\51
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\52
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\53
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\54
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\55
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\56
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\57
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\58
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\59
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\6
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\60
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\61
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\62
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\63
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\7
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\8
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\9
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\host
  Opens:                    C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\muffin
  Opens:                    C:\Documents and Settings\Admin\Application
```

```
Data\Sun\Java\Deployment\cache\6.0\tmp
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\ext
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\log
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\tmp
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\tmp\si
  Opens:                 C:\Documents and Settings\Admin\Application Data\Sun\Java\jre1.7.0_02
  Opens:                 C:\Documents and Settings\Admin\Cookies
  Opens:                 C:\Documents and Settings\Admin\Desktop
  Opens:                 C:\Documents and Settings\Admin\Favorites
  Opens:                 C:\Documents and Settings\Admin\Favorites\Links
  Opens:                 C:\Documents and Settings\Admin\Favorites\Microsoft Websites
  Opens:                 C:\Documents and Settings\Admin\IECompatCache
  Opens:                 C:\Documents and Settings\Admin\IETldCache
  Opens:                 C:\Documents and Settings\Admin\Local Settings
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application Data
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\Search
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Updater
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Color
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\Install
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\CD Burning
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\TLMHA51J
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings\Custom0
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\0WORJP5C
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\LQLIM8KB
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active
```

```
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Services
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Media Player
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\12.0
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\14.0
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\0
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\1
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\10
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\11
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\12
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\13
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\14
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\15
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\16
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\17
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\18
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\19
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\2
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\20
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\21
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\22
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\23
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\24
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\25
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\26
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\27
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\28
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\29
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\3
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\30
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\31
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\32
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\33
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
```

```
Data\Sun\Java\Deployment\cache\6.0\34
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\35
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\36
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\37
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\38
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\39
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\4
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\40
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\41
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\42
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\43
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\44
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\46
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\48
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\49
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\5
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\50
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\51
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\52
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\53
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\54
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\55
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\56
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\57
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\58
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\59
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\6
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\60
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\61
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\62
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\63
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\8
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\9
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\host
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\muffin
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\tmp
  Opens:                 C:\Documents and Settings\Admin\Local Settings\History
  Opens:                 C:\Documents and Settings\Admin\Local Settings\History\History.IE5
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014031220140313
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
```

```
  Opens:                    C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp\gen_py
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_10.0.30319
  Writes to:                C:\WINDOWS\system32\urdvxc.exe
  Reads from:               C:\WINDOWS\Temp\57f19466903ed1ef8c74ef4d8c044ddf.exe
  Reads from:               C:\WINDOWS\system32\urdvxc.exe
  Reads from:               C:\WINDOWS\system32\rsaenh.dll
  Reads from:               C:\WINDOWS\system32\drivers\etc\hosts
  Deletes:                  C:\WINDOWS\Temp\57f19466903ed1ef8c74ef4d8c044ddf.exe
```

Network Events

```
  DNS query:                www.if.ee
  DNS query:                www.online.if.ee
  DNS query:                www.starman.ee
  DNS response:             www.if.ee ⇒ 194.215.38.135
  DNS response:             www.starman.ee ⇒ 62.65.192.24
  DNS response:             www.starman.ee ⇒ 62.65.192.25
  DNS response:             www.online.if.ee ⇒ 195.50.195.10
  Connects to:              63.215.74.195:139
  Connects to:              195.50.195.10:443
  Connects to:              194.215.38.135:80
  Connects to:              62.65.192.25:80
  Connects to:              62.65.192.24:80
  Connects to:              63.215.74.96:139
  Connects to:              63.215.74.195:445
  Connects to:              63.215.74.96:445
  Connects to:              63.215.202.72:139
  Connects to:              63.215.202.72:445
  Sends data to:            8.8.8.8:53
  Sends data to:            0.0.0.0:0
  Sends data to:            www.online.if.ee:443 (195.50.195.10)
  Sends data to:            www.if.ee:80 (194.215.38.135)
  Receives data from:       0.0.0.0:0
  Receives data from:       www.if.ee:80 (194.215.38.135)
  Receives data from:       www.online.if.ee:443 (195.50.195.10)
```

Windows Registry Events

```
  Creates key:              HKCR\clsid\{443b4059-c623-16d3-69c0-1929dfcb80f6}
  Creates key:              HKCR\clsid\{443b4059-c623-16d3-69c0-1929dfcb80f6}\localserver32
  Creates key:              HKCR\clsid\{35349b95-82d3-1178-19ed-0e5d2312f5c0}
  Creates key:              HKCR\clsid\{35349b95-82d3-1178-19ed-0e5d2312f5c0}\localserver32
  Creates key:              HKLM\software\classes
  Creates key:              HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\57f19466903ed1ef8c74ef4d8c044ddf.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                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\image file execution
options\msvcrt.dll
```

```
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  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\shlwapi.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:                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:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  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\software\microsoft\windows nt\currentversion\image file execution
options\icmp.dll
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\clsid\{443b4059-c623-16d3-69c0-1929dfcb80f6}
  Opens key:                HKLM\software\classes
  Opens key:                HKCU\software\classes\clsid\{443b4059-c623-16d3-69c0-
1929dfcb80f6}\localserver32
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  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:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\apphelp.dll
   Opens key:                HKLM\system\wpa\tabletpc
   Opens key:                HKLM\system\wpa\mediacenter
   Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\urdvxc.exe
   Opens key:                HKLM\software\policies\microsoft\windows\safer\levelobjects
   Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
   Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
   Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
   Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
   Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
```

```
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urdvxc.exe
  Opens key:                HKCU\software\classes\clsid\{35349b95-82d3-1178-19ed-0e5d2312f5c0}
  Opens key:                HKCU\software\classes\clsid\{35349b95-82d3-1178-19ed-
0e5d2312f5c0}\localserver32
  Opens key:                HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urdvxc.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKU\.default\software\policies\microsoft\control panel\desktop
  Opens key:                HKU\.default\control panel\desktop
  Opens key:                HKU\.default\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\system\currentcontrolset\control\servicecurrent
  Opens key:                HKU\.default\software\microsoft\cryptography\providers\type 001
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider types\type 001
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
  Opens key:                HKLM\software\microsoft\rpc\securityservice
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  Opens key:                HKLM\software\policies\microsoft\system\dnsclient
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
  Opens key:                HKLM\system\currentcontrolset\services\ldap
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
  Opens key:                HKLM\system\currentcontrolset\control\wmi\security
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
  Opens key:                HKLM\system\currentcontrolset\services\rpc\linkage
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[57f19466903ed1ef8c74ef4d8c044ddf]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[57f19466903ed1ef8c74ef4d8c044ddf]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:            HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:            HKCR\interface[interfacehelperdisableall]
  Queries value:            HKCR\interface[interfacehelperdisableallforole32]
  Queries value:            HKCR\interface[interfacehelperdisabletypelib]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
```

```
   Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:              HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
   Queries value:              HKLM\system\wpa\mediacenter[installed]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
   Queries value:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
   Queries value:              HKLM\software\microsoft\windows
```

```
nt\currentversion\compatibility32[urdvxc]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[urdvxc]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKU\.default\control panel\desktop[multiuilanguageid]
  Queries value:            HKU\.default\control panel\desktop[smoothscroll]
  Queries value:            HKLM\system\currentcontrolset\control\servicecurrent[]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries 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\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
```

```
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
   Queries value:            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
   Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
   Queries value:              HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
   Queries value:              HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
   Sets/Creates value:         HKCR\clsid\{443b4059-c623-16d3-69c0-1929dfcb80f6}[]
   Sets/Creates value:         HKCR\clsid\{443b4059-c623-16d3-69c0-1929dfcb80f6}\localserver32[]
   Sets/Creates value:         HKCR\clsid\{35349b95-82d3-1178-19ed-0e5d2312f5c0}[]
   Sets/Creates value:         HKCR\clsid\{35349b95-82d3-1178-19ed-0e5d2312f5c0}\localserver32[]
   Value changes:              HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:              HKCR\clsid\{35349b95-82d3-1178-19ed-0e5d2312f5c0}[]
   Value changes:              HKCR\clsid\{35349b95-82d3-1178-19ed-0e5d2312f5c0}\localserver32[]
```