Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	821
Risk Level:	7
Date Processed:	2016-05-18 10:42:12 (UTC)
Processing Time:	62.29 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe"

Sample ID:	3328
Type:	basic
Owner:	admin
Label:	6ff8b3dc9a34dc40e47ff4c3444c8241
Date Added:	2016-05-18 10:30:51 (UTC)
File Type:	PE32:win32:gui
File Size:	394240 bytes
MD5:	6ff8b3dc9a34dc40e47ff4c3444c8241
SHA256:	22dd9934836541b81983ef5ed7abb4d82edd6afcdc272f027f8bffb41145fac9
Description:	None

Pattern Matching Results

6	Modifies registry autorun entries
2	PE: Nonstandard section
5	Installs service
7	Disables system restore
5	Adds autostart object
5	PE: Contains compressed section
3	Long sleep detected

Static Events

Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe ["C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\40D10558713B95C1000040D0C48C9AAF
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Creates:	C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF
Creates:	C:\ProgramData\40D10558713B95C1000040D0C48C9AAF
Creates:	C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF.exe
Creates:	C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF.ico
Opens:	C:\Windows\Prefetch\6FF8B3DC9A34DC40E47FF4C3444C8-B42B5CB2.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\activeds.dll
Opens:	C:\Windows\Temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\MSIMG32.dll
Opens:	C:\Windows\System32\msimg32.dll
Opens:	C:\windows\temp\Secur32.dll
Opens:	C:\Windows\System32\secur32.dll
Opens:	C:\windows\temp\SSPICLI.DLL
Opens:	C:\Windows\System32\sspicli.dll
Opens:	C:\windows\temp\WINHTTP.dll
Opens:	C:\Windows\System32\winhttp.dll
Opens:	C:\windows\temp\webio.dll

```
  Opens:                  C:\Windows\System32\webio.dll
  Opens:                  C:\Windows\System32\rpcss.dll
  Opens:                  C:\windows\temp\CRYPTBASE.dll
  Opens:                  C:\Windows\System32\cryptbase.dll
  Opens:                  C:\Windows\System32\uxtheme.dll
  Opens:                  C:\
  Opens:                  C:\windows\temp\profapi.dll
  Opens:                  C:\Windows\System32\profapi.dll
  Opens:
C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF
  Opens:                  C:\ProgramData
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:                  C:\windows\temp\cryptsp.dll
  Opens:                  C:\Windows\System32\cryptsp.dll
  Opens:                  C:\windows\temp\credssp.dll
  Opens:                  C:\Windows\System32\credssp.dll
  Opens:                  C:\Windows\System32\mswsock.dll
  Opens:                  C:\Windows\System32\wshqos.dll
  Opens:                  C:\windows\temp\wshtcpip.DLL
  Opens:                  C:\Windows\System32\WSHTCPIP.DLL
  Opens:                  C:\windows\temp\wship6.dll
  Opens:                  C:\Windows\System32\wship6.dll
  Opens:                  C:\windows\temp\DNSAPI.dll
  Opens:                  C:\Windows\System32\dnsapi.dll
  Opens:                  C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens:                  C:\windows\temp\CRYPTSP.dll
  Opens:                  C:\Windows\System32\rsaenh.dll
  Opens:                  C:\windows\temp\RpcRtRemote.dll
  Opens:                  C:\Windows\System32\RpcRtRemote.dll
  Opens:                  C:\windows\temp\SXS.DLL
  Opens:                  C:\Windows\System32\sxs.dll
  Opens:                  C:\Windows\System32\ieframe.dll
  Opens:                  C:\Windows\System32\stdole2.tlb
  Opens:
C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF.exe
  Opens:                  C:\Windows\System32\tzres.dll
  Opens:                  C:\Windows\System32\en-US\tzres.dll.mui
  Opens:                  C:\Windows\Fonts\arial.ttf
  Opens:                  C:\windows\temp\dwmapi.dll
  Opens:                  C:\Windows\System32\dwmapi.dll
  Opens:                  C:\Windows\system32\uxtheme.dll.Config
  Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
  Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:                  C:\Windows\WindowsShell.Manifest
  Opens:                  C:\Windows\Fonts\arialbd.ttf
  Opens:                  C:\Windows\System32\oleacc.dll
  Opens:                  C:\windows\temp\OLEACCRC.DLL
  Opens:                  C:\Windows\System32\oleaccrc.dll
  Writes to:
C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF.exe
  Writes to:
C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF
  Writes to:
C:\ProgramData\40D10558713B95C1000040D0C48C9AAF\40D10558713B95C1000040D0C48C9AAF.ico
  Reads from:             C:\Windows\System32\activeds.dll
  Reads from:             C:\Windows\Temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Reads from:             C:\Windows\System32\ieframe.dll
  Reads from:             C:\Windows\System32\stdole2.tlb
```

Network Events

```
  Connects to:            175.41.29.181:80
  Sends data to:          175.41.29.181:80
```

Windows Registry Events

```
  Creates key:            HKLM\software\microsoft\security center
  Creates key:            HKLM\software\microsoft\security center\svc
  Creates key:            HKLM\software
  Creates key:            HKLM\software\microsoft
  Creates key:            HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:            HKCU\software\microsoft\windows\currentversion\policies\explorer
  Creates key:            HKLM\system\currentcontrolset\services\luafv
  Creates key:            HKLM\software\microsoft\windows nt\currentversion\systemrestore
  Creates key:            HKLM\software\microsoft\windows\currentversion\policies\system
  Creates key:            HKLM\software\microsoft\windows defender
  Creates key:            HKCU\software\microsoft\windows\currentversion\runonce
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\
  Opens key:                HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                HKLM\software\policies\microsoft\mui\settings
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop\languageconfiguration
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKCU\control panel\desktop\muicached
  Opens key:                HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                HKLM\
  Opens key:                HKLM\system\currentcontrolset\services\crypt32
  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\diagnostics
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}\propertybag
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:                HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\software\microsoft\internet explorer
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\30f56ab0
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
  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\protocol_catalog9\catalog_entries\000000000012
  Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  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\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\connections
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\psched\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\system\currentcontrolset\services\dns
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\treatas
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\progid
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler
  Opens key:                HKCU\software\classes\appid\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens key:                HKCR\appid\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens key:                HKLM\software\microsoft\ole\appcompat
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                  HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                  HKCR\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                  HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                  HKLM\software\microsoft\rpc\extensions
  Opens key:                  HKLM\system\currentcontrolset\services\bfe
  Opens key:                  HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:                  HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key:                  HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
  Opens key:                  HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
  Opens key:                  HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
  Opens key:                  HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
  Opens key:                  HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}
  Opens key:                  HKCR\clsid\{00020424-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
  Opens key:                  HKCR\clsid\{00020424-0000-0000-c000-000000000046}\treatas
  Opens key:                  HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\progid
  Opens key:                  HKCR\clsid\{00020424-0000-0000-c000-000000000046}\progid
  Opens key:                  HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                  HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                  HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                  HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler
  Opens key:                  HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
  Opens key:                  HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
  Opens key:                  HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
  Opens key:                  HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
  Opens key:                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
  Opens key:                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
  Opens key:                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
  Opens key:                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
  Opens key:                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
  Opens key:                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
  Opens key:                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
  Opens key:                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
  Opens key:                  HKCU\software\classes\typelib
  Opens key:                  HKCR\typelib
  Opens key:                  HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                  HKCR\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                  HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                  HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
  Opens key:                  HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
  Opens key:                  HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
  Opens key:                  HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
  Opens key:                  HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                  HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                  HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                  HKCR\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\treatas
  Opens key:                  HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
  Opens key:                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\progid
  Opens key:                  HKCR\clsid\{00020420-0000-0000-c000-000000000046}\progid
  Opens key:                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                  HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                  HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                  HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler
  Opens key:                  HKCU\software\classes\interface\{b196b284-bab4-101a-b69c-00aa00341d07}
  Opens key:                  HKCR\interface\{b196b284-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCU\software\classes\interface\{b196b284-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32
  Opens key:                HKCR\interface\{b196b284-bab4-101a-b69c-00aa00341d07}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCR\interface\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCU\software\classes\interface\{b196b286-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32
  Opens key:                HKCR\interface\{b196b286-bab4-101a-b69c-00aa00341d07}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:
HKLM\software\microsoft\ctf\compatibility\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens key:                HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKLM\software\microsoft\ctf\knownclasses
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:                HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\progid
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[6ff8b3dc9a34dc40e47ff4c3444c8241]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\setup[oobeinprogress]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:            HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[parsingname]
```

```
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[initfolderhandler]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:            HKLM\software\microsoft\internet explorer[version]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing[enabled]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  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\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[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\000000000001[providerinfo]
   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\000000000002[providerinfo]
   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\namespace_catalog5\catalog_entries\000000000003[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
   Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
  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\cmf\config[system]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
  Queries value:          HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
  Queries value:          HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\psched\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[domainnamedevolutionlevel]
 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[screendefaultservers]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 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[dnssecurenamequeryfallback]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 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[addrconfigcontrol]
 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[updatetopleveldomainzones]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
```

```
  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[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:           HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:           HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  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\software\microsoft\com3[com+enabled]
  Queries value:           HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
  Queries value:           HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:           HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:           HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:           HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  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\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:           HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:           HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:           HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:           HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:           HKLM\software\microsoft\cryptography[machineguid]
  Queries value:           HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:           HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:           HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:           HKLM\software\microsoft\sqmclient\windows\disabledprocesses[10b1e396]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:           HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:           HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
  Queries value:           HKCR\clsid\{00020424-0000-0000-c000-000000000046}[]
  Queries value:           HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:           HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:           HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
```

```
  Queries value:              HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
  Queries value:              HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
  Queries value:              HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
  Queries value:              HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
  Queries value:              HKLM\software\microsoft\rpc[udtalignmentpolicy]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{b196b284-bab4-101a-b69c-00aa00341d07}\proxystubclsid32[]
  Queries value:              HKCR\interface\{b196b286-bab4-101a-b69c-00aa00341d07}\proxystubclsid32[]
  Queries value:              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:              HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
  Sets/Creates value:         HKLM\software\microsoft\security center[antivirusoverride]
  Sets/Creates value:         HKLM\software\microsoft\security center[firewalloverride]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[hidescahealth]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\runonce[40d10558713b95c1000040d0c48c9aaf]
  Value changes:              HKLM\software\microsoft\security center[antivirusdisablenotify]
  Value changes:              HKLM\software\microsoft\security center[firewalldisablenotify]
  Value changes:              HKLM\software\microsoft\security center[updatesdisablenotify]
  Value changes:              HKLM\system\currentcontrolset\services\luafv[start]
  Value changes:              HKLM\software\microsoft\windows
nt\currentversion\systemrestore[rpsessioninterval]
  Value changes:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
  Value changes:
HKLM\software\microsoft\windows\currentversion\policies\system[consentpromptbehavioradmin]
  Value changes:              HKLM\software\microsoft\security center[antivirusoverride]
  Value changes:              HKLM\software\microsoft\security center[firewalloverride]
  Value changes:
HKCU\software\microsoft\windows\currentversion\policies\explorer[hidescahealth]
  Value changes:
HKCU\software\microsoft\windows\currentversion\runonce[40d10558713b95c1000040d0c48c9aaf]
```