Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3331, Task ID: 832

Task ID:	832
Risk Level:	10
Date Processed:	2016-05-18 10:44:05 (UTC)
Processing Time:	62.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"
Sample ID:	3331
Type:	basic
Owner:	admin
Label:	1be5bc13fd1cf615a95feec0c5b7fd13
Date Added:	2016-05-18 10:30:52 (UTC)
File Type:	PE32:win32:gui
File Size:	201728 bytes
MD5:	1be5bc13fd1cf615a95feec0c5b7fd13
SHA256:	10e3f54492e5cdcdf2c1ae6d097aafdea9474ff77bf6ccb5a9c762ccb6e4a347
Description:	None

Pattern Matching Results

6 Modifies registry autorun entries
7 Writes to memory of system processes
5 Abnormal sleep detected
5 Installs service
3 Connects to local host
7 Creates file in recycle bin
6 Changes Winsock providers
10 Creates malicious events: ZeroAccess [Rootkit]
4 Reads process memory
7 Opens a recycle bin location
7 Creates threads in system processes
3 Long sleep detected
7 Injects thread into Windows process

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe ["c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"]
Creates process:	C:\WINDOWS\system32\cmd.exe ["C:\WINDOWS\system32\cmd.exe"]
Reads from process:	PID:1988 C:\WINDOWS\system32\calc.exe
Writes to process:	PID:1900 C:\WINDOWS\explorer.exe
Writes to process:	PID:896 C:\WINDOWS\system32\services.exe
Writes to process:	PID:640 C:\WINDOWS\system32\cmd.exe
Terminates process:	C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Creates remote thread:	C:\WINDOWS\explorer.exe
Creates remote thread:	C:\WINDOWS\system32\services.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.EHH
Creates event:	\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates event:	\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000007B4.00000000.00000004
Creates event:	\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000007B4.00000000.00000004
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.ELH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.ELH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.EHH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.EHH.IC
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\RECYCLER
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\L
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\U
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\@
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\n
Creates:	C:\RECYCLER\
Creates:	C:\RECYCLER\S-1-5-18
Creates:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78
Creates:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\L
Creates:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
Creates:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
Creates:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
Creates:	C:GAC_MSIL
Creates:	C:\WINDOWS\assembly\GAC
Creates:	C:\WINDOWS\assembly\GAC\Desktop.ini
Opens:	C:\WINDOWS\Prefetch\1BE5BC13FD1CF615A95FEEC0C5B7F-1D9D4140.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\cabinet.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\mswsock.dll
Opens:	C:\WINDOWS\system32\hnetcfg.dll
Opens:	C:\WINDOWS\system32\wshtcpip.dll
Opens:	C:\WINDOWS\system32\rsaenh.dll
Opens:	C:\WINDOWS\system32\crypt32.dll
Opens:	C:\WINDOWS
Opens:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78
Opens:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\n
Opens:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78
Opens:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
Opens:	C:\WINDOWS\assembly
Opens:	C:\WINDOWS\assembly\GAC\Desktop.ini

Opens:	C:\WINDOWS\assembly\GAC
Opens:	C:\WINDOWS\system32\cmd.exe
Opens:	C:\WINDOWS\system32\apphelp.dll
Opens:	C:\WINDOWS\AppPatch\sysmain.sdb
Opens:	C:\WINDOWS\AppPatch\systest.sdb
Opens:	C:\WINDOWS\system32
Opens:	C:\
Opens:	C:\WINDOWS\system32\cmd.exe.Manifest
Opens:	C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Opens:	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
Opens:	C:
Opens:	C:\WINDOWS\AppPatch
Opens:	C:\WINDOWS\system32\wbem
Opens:	C:\WINDOWS\WinSxS
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\system32\ntdll.dll
Opens:	C:\WINDOWS\system32\kernel32.dll
Opens:	C:\WINDOWS\system32\unicode.nls
Opens:	C:\WINDOWS\system32\locale.nls
Opens:	C:\WINDOWS\system32\sorttbls.nls
Opens:	C:\WINDOWS\system32\msvcrt.dll
Opens:	C:\WINDOWS\system32\user32.dll
Opens:	C:\WINDOWS\system32\gdi32.dll
Opens:	C:\WINDOWS\system32\shimeng.dll
Opens:	C:\WINDOWS\AppPatch\AcGenral.dll
Opens:	C:\WINDOWS\system32\advapi32.dll
Opens:	C:\WINDOWS\system32\rpcrt4.dll
Opens:	C:\WINDOWS\system32\secur32.dll
Opens:	C:\WINDOWS\system32\winmm.dll
Opens:	C:\WINDOWS\system32\ole32.dll
Opens:	C:\WINDOWS\system32\oleaut32.dll
Opens:	C:\WINDOWS\system32\msacm32.dll
Opens:	C:\WINDOWS\system32\version.dll
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\shlwapi.dll
Opens:	C:\WINDOWS\system32\userenv.dll
Opens:	C:\WINDOWS\system32\uxtheme.dll
Opens:	C:\WINDOWS\system32\ctype.nls
Opens:	C:\WINDOWS\system32\sortkey.nls
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\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\wbem\wmic.exe
Opens:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
Opens:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\@
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Config
Opens:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
Opens:	C:\WINDOWS\Temp\477ed5dc-1e37-4928-b33b-364159e99071
Opens:	C:\WINDOWS\system32\calc.exe
Opens:	C:\WINDOWS\system32\drprov.dll
Opens:	C:\WINDOWS\system32\ntlanman.dll
Opens:	C:\WINDOWS\system32\netui0.dll
Opens:	C:\WINDOWS\system32\netui1.dll
Opens:	C:\WINDOWS\system32\netrap.dll
Opens:	C:\WINDOWS\system32\samlib.dll
Opens:	C:\WINDOWS\system32\davclnt.dll
Opens:	C:\WINDOWS\system32\MSIMTF.dll
Writes to:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\@
Writes to:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\n
Writes to:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
Writes to:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
Writes to:	C:\WINDOWS\assembly\GAC\Desktop.ini
Reads from:	C:\WINDOWS\system32\rsaenh.dll
Reads from:	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
Reads from:	C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
Reads from:	C:\WINDOWS\system32\calc.exe
Deletes:	C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe

Network Events

DNS query:	j.maxmind.com
DNS response:	j.maxmind.com ⇒ 127.0.0.1
Connects to:	127.0.0.1:80
Sends data to:	8.8.8.8:53
Sends data to:	83.133.123.20:53
Sends data to:	68.185.188.253:16471
Sends data to:	189.68.16.1:16471
Sends data to:	109.53.87.1:16471
Sends data to:	68.49.152.252:16471
Sends data to:	80.109.74.3:16471
Sends data to:	130.204.226.4:16471
Sends data to:	221.244.148.250:16471
Sends data to:	176.227.128.250:16471
Sends data to:	173.80.73.5:16471
Sends data to:	74.210.157.7:16471
Sends data to:	180.47.189.7:16471
Sends data to:	74.56.221.248:16471
Sends data to:	37.192.19.8:16471
Sends data to:	68.119.104.8:16471
Sends data to:	98.200.249.8:16471
Sends data to:	37.4.80.10:16471
Sends data to:	187.14.203.11:16471
Sends data to:	68.16.8.248:16471
Sends data to:	176.200.253.13:16471
Sends data to:	72.177.97.245:16471
Sends data to:	77.0.111.14:16471
Sends data to:	174.5.197.15:16471
Sends data to:	76.24.211.244:16471
Sends data to:	70.119.200.15:16471
Sends data to:	108.129.22.18:16471
Sends data to:	96.30.133.20:16471
Sends data to:	67.163.238.20:16471
Sends data to:	72.204.20.22:16471
Sends data to:	190.219.25.242:16471

Sends data to: 98.121.198.241:16471
Sends data to: 200.127.18.241:16471
Sends data to: 79.114.143.240:16471
Sends data to: 217.209.199.22:16471
Sends data to: 180.31.88.23:16471
Sends data to: 77.103.179.238:16471
Sends data to: 146.247.84.238:16471
Sends data to: 124.123.122.236:16471
Sends data to: 69.204.104.236:16471
Sends data to: 98.196.20.25:16471
Sends data to: 109.192.63.25:16471
Sends data to: 151.43.129.233:16471
Sends data to: 97.106.93.233:16471
Sends data to: 61.192.120.25:16471
Sends data to: 68.35.204.26:16471
Sends data to: 75.74.160.229:16471
Sends data to: 190.178.170.27:16471
Sends data to: 95.223.50.224:16471
Sends data to: 174.134.97.223:16471
Receives data from: 0.0.0.0:0

Windows Registry Events

Creates key: HKCU\software\classes\clsid
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32
Creates key: HKLM\software\clients\startmenuinternet
Creates key: HKCR\http\shell
Creates key: HKCU\software\microsoft\multimedia\audio
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00
Creates key: HKCU\sessioninformation
Deletes value: HKLM\software\microsoft\windows\currentversion\run[windows defender]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
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\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\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key: HKLM\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\currentversion\explorer\performance
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
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\cabinet.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2help.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key: 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\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\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\1be5bc13fd1cf615a95feec0c5b7fd13.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
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\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
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\cryptography\deshashsessionkeybackward
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\n
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-
9a6f-135d9c6622cc}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-aa9d-4618-
a949-c1b91af43b1a}
Opens key: HKLM\software\microsoft\windows\currentversion\run
Opens key: HKLM\software\microsoft\com3
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\treatas
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprocserver32
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserver32
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprocserverx86
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\localserver32
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver32
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandler32
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler32
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandlerx86
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\localserver
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver
Opens key: HKCU\software\classes\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
Opens key: HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\treatas
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserver32
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserverx86
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\localserver32
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver32
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandler32
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandlerx86
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\localserver
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver
Opens key: HKCU\software\classes\http
Opens key: HKCR\http
Opens key: HKCU\software\classes\http\curver
Opens key: HKCR\http\curver
Opens key: HKCR\http\
Opens key: HKCU\software\classes\http\shell\open
Opens key: HKCR\http\shell\open
Opens key: HKCU\software\classes\http\shell\open\command
Opens key: HKCR\http\shell\open\command
Opens key: HKCU\software\classes\http\shell
Opens key: HKLM\software\classes
Opens key: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_ntfs\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_ntfs\0000\root&legacy_ntfs&0000

Opens key: HKLM\system\currentcontrolset\enum\root\legacy_null\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_null\0000\root&legacy_null&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_partmgr\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_partmgr\0000\root&legacy_partmgr&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_parvdm\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_parvdm\0000\root&legacy_parvdm&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_policyagent\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_policyagent\0000\root&legacy_policyagent&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_protectedstorage\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_protectedstorage\0000\root&legacy_protectedstorage&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rasacd\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rasacd\0000\root&legacy_rasacd&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rasman\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rasman\0000\root&legacy_rasman&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rdbss\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rdbss\0000\root&legacy_rdbss&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rdpcdd\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rdpcdd\0000\root&legacy_rdpcdd&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rdpnp\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rdpnp\0000\root&legacy_rdpnp&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rdpwd\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rdpwd\0000\root&legacy_rdpwd&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_remoteregistry\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_remoteregistry\0000\root&legacy_remoteregistry&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rpcss\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rpcss\0000\root&legacy_rpcss&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_samss\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_samss\0000\root&legacy_samss&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_schedule\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_schedule\0000\root&legacy_schedule&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_seclogon\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_seclogon\0000\root&legacy_seclogon&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_sens\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_sens\0000\root&legacy_sens&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_serial\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_serial\0000\root&legacy_serial&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_sharedaccess\0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_shellhwdetection\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_shellhwdetection\0000\root&legacy_shellhwdetection&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_snetmon\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_snetmon\0000\root&legacy_snetmon&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_spooler\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_spooler\0000\root&legacy_spooler&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_sprocmon\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_sprocmon\0000\root&legacy_sprocmon&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_sr\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_sr\0000\root&legacy_sr&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_sregmon\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_sregmon\0000\root&legacy_sregmon&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_srootkit\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_srootkit\0000\root&legacy_srootkit&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_srservice\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_srservice\0000\root&legacy_srservice&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_srv\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_srv\0000\root&legacy_srv&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_ssdpsrv\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_ssdpsrv\0000\root&legacy_ssdpsrv&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_stisvc\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_stisvc\0000\root&legacy_stisvc&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_tapisrv\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_tapisrv\0000\root&legacy_tapisrv&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_tcpip\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_tcpip\0000\root&legacy_tcpip&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_tdtcp\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_tdtcp\0000\root&legacy_tdtcp&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_termservice\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_termservice\0000\root&legacy_termservice&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_themes\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_themes\0000\root&legacy_themes&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_tlntsvr\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_tlntsvr\0000\root&legacy_tlntsvr&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_trkwks\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_trkwks\0000\root&legacy_trkwks&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_vga\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_vga\0000\root&legacy_vga&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_vgasave\0000

Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_vgasave\0000\root&legacy_vgasave&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_volsnap\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_volsnap\0000\root&legacy_volsnap&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_w32time\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_w32time\0000\root&legacy_w32time&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_wanarp\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_wanarp\0000\root&legacy_wanarp&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_webclient\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_webclient\0000\root&legacy_webclient&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_winmgmt\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_winmgmt\0000\root&legacy_winmgmt&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_wscsvc\0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_wuauserv\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_wuauserv\0000\root&legacy_wuauserv&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_wzcsvc\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_wzcsvc\0000\root&legacy_wzcsvc&0000
Opens key: HKLM\system\currentcontrolset\enum\root\media\ms_mmacm
Opens key:
HKLM\system\currentcontrolset\enum\root\media\ms_mmacm\root&media&ms_mmacm
Opens key: HKLM\system\currentcontrolset\enum\root\media\ms_mmdrv
Opens key:
HKLM\system\currentcontrolset\enum\root\media\ms_mmdrv\root&media&ms_mmdrv
Opens key: HKLM\system\currentcontrolset\enum\root\media\ms_mmmci
Opens key:
HKLM\system\currentcontrolset\enum\root\media\ms_mmmci\root&media&ms_mmmci
Opens key: HKLM\system\currentcontrolset\enum\root\media\ms_mmvcd
Opens key:
HKLM\system\currentcontrolset\enum\root\media\ms_mmvcd\root&media&ms_mmvcd
Opens key: HKLM\system\currentcontrolset\enum\root\media\ms_mmvid
Opens key:
HKLM\system\currentcontrolset\enum\root\media\ms_mmvid\root&media&ms_mmvid
Opens key: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000\root&ms_l2tpminiport&0000
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000\root&ms_ndiswanip&0000
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000\root&ms_pppoeminiport&0000
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000\root&ms_pptpminiport&0000
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0000\root&ms_pschedmp&0000
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001
Opens key:
HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001\root&ms_pschedmp&0001
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ptiminiport\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\ms_ptiminiport\0000\root&ms_ptiminiport&0000
Opens key: HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0000
Opens key:
HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0000\root&nnetsec_mp&0000
Opens key: HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0001
Opens key:
HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0001\root&nnetsec_mp&0001
Opens key: HKLM\system\currentcontrolset\enum\root\rdpdr\0000
Opens key: HKLM\system\currentcontrolset\enum\root\rdpdr\0000\root&rdpdr&0000
Opens key: HKLM\system\currentcontrolset\enum\root\rdp_kbd\0000
Opens key: HKLM\system\currentcontrolset\enum\root\rdp_kbd\0000\root&rdp_kbd&0000
Opens key: HKLM\system\currentcontrolset\enum\root\rdp_mou\0000
Opens key: HKLM\system\currentcontrolset\enum\root\rdp_mou\0000\root&rdp_mou&0000
Opens key: HKLM\system\currentcontrolset\enum\root\system\0000
Opens key: HKLM\system\currentcontrolset\enum\root\system\0000\root&system&0000
Opens key: HKLM\system\currentcontrolset\enum\root\system\0001
Opens key: HKLM\system\currentcontrolset\enum\root\system\0001\root&system&0001
Opens key: HKLM\system\currentcontrolset\enum\root\system\0002
Opens key: HKLM\system\currentcontrolset\enum\root\system\0002\root&system&0002
Opens key:
HKLM\system\currentcontrolset\enum\storage\volume\1&30a96598&0&signaturea045a045offset7e00length78aa94600
Opens key:
HKLM\system\currentcontrolset\enum\storage\volume\1&30a96598&0&signaturea045a045offset7e00length78aa94600\storage&volume&1&30a96598&0&signaturea045a045offset7e00length78aa94600
Opens key: HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac
Opens key: HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac\sw&{eeab7790-c514-11d1-b42b-00805fc1270e}&asyncmac
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18\pci&ven_1022&dev_2000&subsys_20001022&rev_40&3&267a616a&0&18
Opens key: HKCU\software\policies\microsoft\windows\network connections
Opens key: HKLM\software\policies\microsoft\windows\network connections
Opens key: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder
Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{2227a280-3aea-1069-
a2de-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}\shellfolder
Opens key: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\
Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder

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\currentversion\explorer\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cmd.exe
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
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\microsoft\windows nt\currentversion\profilelist\s-1-5-19
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\cmd.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\acgenral.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shimeng.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winmm.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msacm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\userenv.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uxtheme.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
Opens key: HKLM\system\setup
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\system\currentcontrolset\control\productoptions
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\system\currentcontrolset\services\sharedaccess
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
Opens key: HKLM\software\microsoft\ctf\tip\
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mpr.dll
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\system\currentcontrolset
Opens key: HKLM\system\currentcontrolset\services\rdpnp\networkprovider
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider
Opens key: HKLM\system\currentcontrolset\services\webclient\networkprovider
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\drprov.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netui0.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\network\world full access shared parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netrap.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\samlib.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netui1.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntlanman.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\davclnt.dll
Opens key: HKCU\network
Opens key: HKCU\appevents\schemes\apps\.default\systemnotification\.current
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[1be5bc13fd1cf615a95feec0c5b7fd13]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[1be5bc13fd1cf615a95feec0c5b7fd13]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
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\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\software\microsoft\rpc[maxrpcsize]
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\control\computername\activecomputername[computername]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base cryptographic provider v1.0[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base cryptographic provider v1.0[image path]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]

Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[appid]
Queries value: HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[dllsurrogate]
Queries value: HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[localservice]
Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]
Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[appid]
Queries value: HKCR\http\shell\open\command[]
Queries value: HKLM\software\clients\startmenuinternet[]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_null\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_partmgr\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_parvdm\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_rasacd\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_rdpcdd\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_rdpwd\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_serial\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_snetmon\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_sprocmon\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_sregmon\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_srootkit\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_tcpip\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_tdtcp\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_vgasave\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_volsnap\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_wanarp\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\media\ms_mmacm[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\media\ms_mmdrv[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\media\ms_mmmci[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\media\ms_mmvcd[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\media\ms_mmvid[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[classguid]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ptiminiport\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0001[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\rdpdr\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\rdp_kbd\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\rdp_mou\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\system\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\system\0001[classguid]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
Queries value: HKLM\system\currentcontrolset\enum\root\system\0002[classguid]
Queries value: HKLM\system\currentcontrolset\enum\storage\volume\1&30a96598&0&signaturea045a045offset7e00length78aa9460 0[classguid]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18[driver]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18[capabilities]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18[configflags]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18[classguid]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18[friendlyname]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18[devicedesc]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ptiminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0001[driver]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder[attributes]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder[callforattributes]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{2227a280-3aea-1069-a2de-08002b30309d}]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll,-9319]
Queries value: HKLM\system\currentcontrolset\control\session manager\appcompatibility[disableappcompat]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder[attributes]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{7007acc7-3202-11d1-aad2-00805fc1270e}]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\netshell.dll,-1200]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19[refcount]
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[cmd]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]

Queries value: HKCU\software\microsoft\multimedia\audio[systemformats]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.imaadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg711]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.trspch]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl_anet]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
Queries value: HKCU\software\microsoft\multimedia\audio compression manager\msacm[nopcmconverter]
Queries value: HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00[priority1]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[chkaccdebuglevel]
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[personal]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local settings]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsopdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[start]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
Queries value: HKLM\system\currentcontrolset\control\networkprovider\hworder[providerorder]
Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[name]
Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[class]
Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[providerpath]
Queries value: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[name]
Queries value: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[class]
Queries value: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[providerpath]
Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[name]
Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[class]
Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[providerpath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\network\world full access shared parameters[sort hyphens]
Queries value: HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32[]
Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Value changes: HKCU\sessioninformation[programcount]