Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2453
Risk Level:	6
Date Processed:	2016-02-22 05:32:02 (UTC)
Processing Time:	5.06 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe"

Sample ID:	627
Type:	basic
Owner:	admin
Label:	d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174
Date Added:	2016-02-22 05:26:50 (UTC)
File Type:	PE32:win32:gui
File Size:	327744 bytes
MD5:	08c1a0627200a235be2709d4ef702f3f
SHA256:	d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
6	Dumps and runs batch script
4	Terminates process under Windows subfolder
4	Self-delete batch script

Static Events

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

Process/Thread Events

Creates process:	C:\windows\temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe ["C:\windows\temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe"]
Creates process:	C:\Windows\SysWOW64\cmd.exe [cmd /c C:\Users\Admin\AppData\Local\Temp\nskmstc.bat]
Creates process:	\SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe 0xffffffff]
Creates process:	C:\Users\Admin\AppData\Local\Temp\cdlnfb.exe ["C:\Users\Admin\AppData\Local\Temp\cdlnfb.exe"]
Creates process:	C:\Windows\SysWOW64\PING.EXE [ping 127.0.0.1]
Terminates process:	C:\Windows\Temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe
Terminates process:	C:\Users\Admin\AppData\Local\Temp\cdlnfb.exe
Terminates process:	C:\Windows\SysWOW64\PING.EXE
Terminates process:	C:\Windows\SysWOW64\cmd.exe
Terminates process:	C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\cdlnfb.exe
Creates:	C:\Users\Admin\AppData\Local\Temp\aienxg.bat
Creates:	C:\Users\Admin\AppData\Local\Temp\nskmstc.bat
Opens:	C:\Windows\Prefetch\D488539402ABAE3873B801373DBC8-24AF8C8A.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll

Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\iertutil.dll
Opens:	C:\Windows\SysWOW64\wininet.dll
Opens:	C:\Windows\SysWOW64\urlmon.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\Windows\SysWOW64\tzres.dll
Opens:	C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Users\Admin\AppData\Local\Temp\nskmstc.bat
Opens:	C:\Users\Admin\AppData\Local\Temp
Opens:	C:\
Opens:	C:\Users
Opens:	C:\Users\Admin
Opens:	C:\Users\Admin\AppData
Opens:	C:\Users\Admin\AppData\Local
Opens:	C:\Windows\SysWOW64\cmd.exe
Opens:	C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Opens:	C:
Opens:	C:\Windows\Globalization
Opens:	C:\Windows\Globalization\Sorting
Opens:	C:\Windows\System32
Opens:	C:\Windows\SysWOW64\wbem
Opens:	C:\Windows\System32\ntdll.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\System32\kernel32.dll
Opens:	C:\Windows\System32\user32.dll
Opens:	C:\Windows\System32\locale.nls
Opens:	C:\Windows\SysWOW64\wbem\WMIC.exe
Opens:	C:\Windows\System32\conhost.exe
Opens:	C:\Windows\System32\combase.dll
Opens:	C:\Windows\System32\en-US\conhost.exe.mui
Opens:	C:\Windows\System32\ole32.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\Windows\System32\cmd.exe
Opens:	C:\Windows\System32\en-US\cmd.exe.mui
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\system32\uxtheme.dll.Config
Opens:	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
Opens:	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\System32\SHCore.dll
Opens:	C:\Windows\SysWOW64\cmdext.dll
Opens:	C:\Users\Admin\AppData\Local\Temp\nskmstc.bat\
Opens:	C:\Users\Admin\AppData\Local\Temp\aienxg.bat
Opens:	C:\Users\Admin\AppData\Local\Temp\ovsoicof.bat
Opens:	C:\Users\Admin\AppData\Local\Temp\ovsoicof.bat\
Opens:	C:\Users\Admin\AppData\Local\Temp\cdlnfb.exe
Opens:	C:\Windows\Prefetch\CDLNFB.EXE-857B55B3.pf
Opens:	C:\Windows\SysWOW64\dbghelp.dll
Opens:	C:\Windows\SysWOW64\PING.EXE
Opens:	C:\Windows\Prefetch\PING.EXE-371F41E2.pf
Opens:	C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\Windows\SysWOW64\nsi.dll
Opens:	C:\Windows\SysWOW64\ws2_32.dll
Opens:	C:\Windows\SysWOW64\mswsock.dll
Opens:	C:\Windows\SysWOW64\en-US\ping.exe.mui
Opens:	C:\Windows\Temp
Opens:	C:\Windows\SysWOW64\en-US\cmd.exe.mui
Writes to:	C:\Users\Admin\AppData\Local\Temp\cdlnfb.exe
Writes to:	C:\Users\Admin\AppData\Local\Temp\aienxg.bat
Writes to:	C:\Users\Admin\AppData\Local\Temp\nskmstc.bat
Reads from:	C:\Users\Admin\AppData\Local\Temp\nskmstc.bat
Reads from:	C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Reads from:	C:\Users\Admin\AppData\Local\Temp\aienxg.bat
Reads from:	C:\Users\Admin\AppData\Local\Temp\cdlnfb.exe
Reads from:	C:\Windows\SysWOW64\PING.EXE
Deletes:	C:\Users\Admin\AppData\Local\Temp\aienxg.bat

Windows Registry Events

Creates key:	HKLM\software\wow6432node\microsoft\windows\currentversion\datetime

```
  Opens key:                 HKLM\software\microsoft\wow64
  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\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                 HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                 HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                 HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                 HKLM\system\currentcontrolset\control\nls\language
  Opens key:                 HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:                 HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:                 HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:                 HKLM\software\policies\microsoft\mui\settings
  Opens key:                 HKCU\
  Opens key:                 HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                 HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  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\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:                 HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:                 HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key:                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:                 HKLM\
  Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:                 HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                 HKLM\software\wow6432node\microsoft\ole
  Opens key:                 HKLM\software\microsoft\ole
  Opens key:                 HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                 HKLM\software\microsoft\ole\tracing
  Opens key:                 HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                 HKLM\software\microsoft\sqmclient\windows
  Opens key:                 HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                 HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                 HKLM\system\currentcontrolset\control\session manager
  Opens key:                 HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                 HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                 HKCU\software\microsoft\internet explorer\main
  Opens key:                 HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\windows\appcompat
  Opens key:                 HKLM\software\policies\microsoft\windows\appcompat
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                 HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\nskmstc.bat
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
  Opens key:                 HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\conhost.exe
  Opens key:                 HKLM\software\microsoft\windows\currentversion\sidebyside
  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\oleaut
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\console\truetypefont
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\console\fullscreen
  Opens key:                 HKCU\console
```

```
 Opens key:                 HKCU\console\
 Opens key:                 HKCU\console\%systemroot%_system32_cmd.exe
 Opens key:                 HKCU\console\%systemroot%\system32\cmd.exe
 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:                 HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
 Opens key:                 HKLM\software\microsoft\ctf\compatibility\conhost.exe
 Opens key:                 HKLM\software\microsoft\windows\windows error reporting\wmr
 Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\explorer
 Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\explorer
 Opens key:                 HKCU\software\policies\microsoft\windows\system
 Opens key:                 HKLM\software\wow6432node\microsoft\command processor
 Opens key:                 HKCU\software\microsoft\command processor
 Opens key:                 HKLM\software\wow6432node\policies\microsoft\windows\safer\levelobjects
 Opens key:                 HKLM\software\policies\microsoft\windows\safer\levelobjects
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\0\paths
 Opens key:                 HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\0\hashes
 Opens key:                 HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\4096\paths
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\65536\paths
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\131072\paths
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\262144\paths
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
 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:                HKLM\system\currentcontrolset\control\srp\gp\
  Opens key:                HKLM\system\currentcontrolset\control\srp\gp
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cdlnfb.exe
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cdlnfb.exe
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ping.exe
  Opens key:                HKCU\software\microsoft\windows nt\currentversion
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\ping.exe
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\ping.exe
  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\111cc00d-1058ed91
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\111cc00d
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
  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\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
  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\services\tcpip\parameters
   Opens key:                HKLM\software\wow6432node\microsoft\rpc
   Opens key:                HKLM\software\microsoft\rpc
   Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:                HKLM\system\setup
   Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
   Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
   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:            HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
   Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
   Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
   Queries value:            HKCU\control panel\desktop[preferreduilanguages]
   Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe]
   Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174]
   Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
   Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
   Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
   Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
   Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
   Queries value:            HKCU\software\microsoft\internet explorer\main[start page]
   Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
   Queries value:            HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Queries value:            HKCU\console[screencolors]
   Queries value:            HKCU\console[popupcolors]
   Queries value:            HKCU\console[insertmode]
   Queries value:            HKCU\console[quickedit]
   Queries value:            HKCU\console[codepage]
   Queries value:            HKCU\console[screenbuffersize]
   Queries value:            HKCU\console[windowsize]
   Queries value:            HKCU\console[windowposition]
   Queries value:            HKCU\console[fontsize]
   Queries value:            HKCU\console[fontfamily]
   Queries value:            HKCU\console[fontweight]
   Queries value:            HKCU\console[facename]
   Queries value:            HKCU\console[cursorsize]
   Queries value:            HKCU\console[historybuffersize]
   Queries value:            HKCU\console[numberofhistorybuffers]
```

```
  Queries value:          HKCU\console[historynodup]
  Queries value:          HKCU\console[colortable00]
  Queries value:          HKCU\console[colortable01]
  Queries value:          HKCU\console[colortable02]
  Queries value:          HKCU\console[colortable03]
  Queries value:          HKCU\console[colortable04]
  Queries value:          HKCU\console[colortable05]
  Queries value:          HKCU\console[colortable06]
  Queries value:          HKCU\console[colortable07]
  Queries value:          HKCU\console[colortable08]
  Queries value:          HKCU\console[colortable09]
  Queries value:          HKCU\console[colortable10]
  Queries value:          HKCU\console[colortable11]
  Queries value:          HKCU\console[colortable12]
  Queries value:          HKCU\console[colortable13]
  Queries value:          HKCU\console[colortable14]
  Queries value:          HKCU\console[colortable15]
  Queries value:          HKCU\console[loadconime]
  Queries value:          HKCU\console[extendededitkey]
  Queries value:          HKCU\console[extendededitkeycustom]
  Queries value:          HKCU\console[worddelimiters]
  Queries value:          HKCU\console[trimleadingzeros]
  Queries value:          HKCU\console[enablecolorselection]
  Queries value:          HKCU\console[scrollscale]
  Queries value:          HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:          HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
  Queries value:          HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
  Queries value:          HKLM\software\wow6432node\microsoft\command processor[disableunccheck]
  Queries value:          HKLM\software\wow6432node\microsoft\command processor[enableextensions]
  Queries value:          HKLM\software\wow6432node\microsoft\command processor[delayedexpansion]
  Queries value:          HKLM\software\wow6432node\microsoft\command processor[defaultcolor]
  Queries value:          HKLM\software\wow6432node\microsoft\command processor[completionchar]
  Queries value:          HKLM\software\wow6432node\microsoft\command
processor[pathcompletionchar]
  Queries value:          HKLM\software\wow6432node\microsoft\command processor[autorun]
  Queries value:          HKCU\software\microsoft\command processor[disableunccheck]
  Queries value:          HKCU\software\microsoft\command processor[enableextensions]
  Queries value:          HKCU\software\microsoft\command processor[delayedexpansion]
  Queries value:          HKCU\software\microsoft\command processor[defaultcolor]
  Queries value:          HKCU\software\microsoft\command processor[completionchar]
  Queries value:          HKCU\software\microsoft\command processor[pathcompletionchar]
  Queries value:          HKCU\software\microsoft\command processor[autorun]
  Queries value:          HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[saferflags]
  Queries value:          HKLM\system\currentcontrolset\control\srp\gp[rulecount]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[cdlnfb.exe]
  Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[cdlnfb]
  Queries value:          HKLM\software\wow6432node\microsoft\internet explorer[version]
  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\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\tcpip\parameters[defaultttl]
  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\rpc[idletimerwindow]
  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\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]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\datetime[index]
```