Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 627, Task ID: 2455

Task ID:	2455
Risk Level:	6
Date Processed:	2016-02-22 05:32:31 (UTC)
Processing Time:	8.41 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

4	Terminates process under Windows subfolder
6	Dumps and runs batch script
2	PE: Nonstandard section
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\system32\cmd.exe [cmd /c C:\Users\Admin\AppData\Local\Temp\mlewbms.bat]
Creates process:	C:\Users\Admin\AppData\Local\Temp\vplhww.exe ["C:\Users\Admin\AppData\Local\Temp\vplhww.exe"]
Creates process:	C:\Windows\system32\PING.EXE [ping 127.0.0.1]
Terminates process:	C:\Windows\Temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe
Terminates process:	C:\Users\Admin\AppData\Local\Temp\vplhww.exe
Terminates process:	C:\Windows\System32\PING.EXE
Terminates process:	C:\Windows\System32\cmd.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\ConsoleEvent-0x00000A58

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\vplhww.exe
Creates:	C:\Users\Admin\AppData\Local\Temp\zpyati.bat
Creates:	C:\Users\Admin\AppData\Local\Temp\mlewbms.bat
Opens:	C:\Windows\Prefetch\D488539402ABAE3873B801373DBC8-24AF8C8A.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\System32\tzres.dll
Opens:	C:\Windows\System32\en-US\tzres.dll.mui
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Users\Admin\AppData\Local\Temp\mlewbms.bat
Opens:	C:\Windows\System32\apphelp.dll
Opens:	C:\Windows\AppPatch\sysmain.sdb
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\temp\cmd.exe
Opens:	C:\Windows\System32\cmd.exe
Opens:	C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
Opens:	C:

```
  Opens:                  C:\Program Files
  Opens:                  C:\Program Files\Adobe
  Opens:                  C:\Program Files\Adobe\Reader 9.0
  Opens:                  C:\Program Files\Adobe\Reader 9.0\Reader
  Opens:                  C:\Windows
  Opens:                  C:\Windows\Branding
  Opens:                  C:\Windows\Branding\Basebrd
  Opens:                  C:\Windows\Branding\Basebrd\en-US
  Opens:                  C:\Windows\Globalization
  Opens:                  C:\Windows\Globalization\Sorting
  Opens:                  C:\Windows\System32\en-US
  Opens:                  C:\Windows\System32\ntdll.dll
  Opens:                  C:\Windows\System32\kernel32.dll
  Opens:                  C:\Windows\System32\apisetschema.dll
  Opens:                  C:\Windows\System32\KernelBase.dll
  Opens:                  C:\Windows\System32\locale.nls
  Opens:                  C:\Windows\System32\msvcrt.dll
  Opens:                  C:\Windows\System32\winbrand.dll
  Opens:                  C:\Windows\System32\user32.dll
  Opens:                  C:\Windows\System32\gdi32.dll
  Opens:                  C:\Windows\System32\lpk.dll
  Opens:                  C:\Windows\System32\usp10.dll
  Opens:                  C:\Windows\System32\msctf.dll
  Opens:                  C:\Windows\System32\en-US\cmd.exe.mui
  Opens:                  C:\Windows\Branding\Basebrd\basebrd.dll
  Opens:                  C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
  Opens:                  C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
  Opens:                  C:\Users\Admin\AppData\Local\Temp\mlewbms.bat\
  Opens:                  C:\Users\Admin\AppData\Local\Temp\zpyati.bat
  Opens:                  C:\Users\Admin\AppData\Local\Temp\qotccgus.bat
  Opens:                  C:\Users\Admin\AppData\Local\Temp\qotccgus.bat\
  Opens:                  C:\Windows\system32\"C:\Users\Admin\AppData\Local\Temp\vplhww.exe"
  Opens:                  C:\Users\Admin\AppData\Local\Temp\vplhww.exe
  Opens:                  C:\Users\Admin\AppData\Local\Temp\ui\SwDRM.dll
  Opens:                  C:\Windows\Prefetch\VPLHWW.EXE-E190B2CE.pf
  Opens:                  C:\Users\Admin\AppData\Local\Temp\dbghelp.dll
  Opens:                  C:\Windows\System32\dbghelp.dll
  Opens:                  C:\Users\Admin\AppData\Local\Temp\dwmapi.dll
  Opens:                  C:\Windows\System32\PING.EXE
  Opens:                  C:\Windows\system32\ui\SwDRM.dll
  Opens:                  C:\Windows\Prefetch\PING.EXE-7E94E73E.pf
  Opens:                  C:\Windows\System32\IPHLPAPI.DLL
  Opens:                  C:\Windows\System32\winnsi.dll
  Opens:                  C:\Windows\System32\en-US\ping.exe.mui
  Opens:                  C:\Windows\System32\mswsock.dll
  Opens:                  C:\Windows\System32\wshqos.dll
  Opens:                  C:\Windows\System32\WSHTCPIP.DLL
  Opens:                  C:\Windows\System32\wship6.dll
  Opens:
C:\Windows\Temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe
  Opens:                  C:\Windows\Temp
  Writes to:              C:\Users\Admin\AppData\Local\Temp\vplhww.exe
  Writes to:              C:\Users\Admin\AppData\Local\Temp\zpyati.bat
  Writes to:              C:\Users\Admin\AppData\Local\Temp\mlewbms.bat
  Reads from:             C:\Users\Admin\AppData\Local\Temp\mlewbms.bat
  Reads from:             C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Reads from:             C:\Users\Admin\AppData\Local\Temp\zpyati.bat
  Reads from:             C:\Users\Admin\AppData\Local\Temp\vplhww.exe
  Reads from:             C:\Windows\System32\PING.EXE
  Deletes:                C:\Users\Admin\AppData\Local\Temp\zpyati.bat
  Deletes:
C:\Windows\Temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe
  Deletes:                C:\Users\Admin\AppData\Local\Temp\mlewbms.bat
```

Windows Registry Events

```
  Creates key:            HKLM\software\microsoft\windows\currentversion\datetime
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\
  Opens key:              HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:              HKLM\software\policies\microsoft\mui\settings
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:              HKCU\control panel\desktop\languageconfiguration
  Opens key:              HKCU\control panel\desktop
  Opens key:              HKCU\control panel\desktop\muicached
  Opens key:              HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\versions
  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\
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:               HKLM\software\microsoft\ole
  Opens key:               HKLM\software\microsoft\ole\tracing
  Opens key:               HKLM\software\microsoft\oleaut
  Opens key:               HKLM\system\currentcontrolset\services\crypt32
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:               HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:               HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:               HKLM\system\currentcontrolset\control\cmf\config
  Opens key:               HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:               HKCU\software\microsoft\internet explorer\main
  Opens key:               HKLM\system\currentcontrolset\control\session manager\appcompatibility
  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\mlewbms.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
  Opens key:               HKCU\software\policies\microsoft\windows\system
  Opens key:               HKLM\software\microsoft\command processor
  Opens key:               HKCU\software\microsoft\command processor
  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\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\hashes
  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:                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\vplhww.exe
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\vplhww.exe
  Opens key:                HKLM\software\microsoft\internet explorer
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ping.exe
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\ping.exe
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  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\143b4853-1058ed91
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\143b4853
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\psched\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  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\cmf\config[system]
  Queries value:            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  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
nt\currentversion\appcompatflags\layers[c:\users\admin\appdata\local\temp\mlewbms.bat]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
  Queries value:            HKLM\software\microsoft\command processor[disableunccheck]
  Queries value:            HKLM\software\microsoft\command processor[enableextensions]
  Queries value:            HKLM\software\microsoft\command processor[delayedexpansion]
  Queries value:            HKLM\software\microsoft\command processor[defaultcolor]
  Queries value:            HKLM\software\microsoft\command processor[completionchar]
  Queries value:            HKLM\software\microsoft\command processor[pathcompletionchar]
  Queries value:            HKLM\software\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\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[1]
  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\appcompatflags\layers[c:\users\admin\appdata\local\temp\vplhww.exe]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[vplhww]
  Queries value:             HKLM\software\microsoft\internet explorer[version]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\windows\system32\ping.exe]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\compatibility32[ping]
  Queries value:             HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Queries value:              HKLM\system\currentcontrolset\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\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
   Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
   Queries value:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
   Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[minsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[maxsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[usedelayedacceptance]
   Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[helperdllname]
   Sets/Creates value:         HKLM\software\microsoft\windows\currentversion\datetime[index]
```