Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3312, Task ID: 757

Task ID: 757 Risk Level: 10

Date Processed: 2016-05-18 10:34:22 (UTC)

Processing Time: 65.88 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"

Sample ID: 3312 Type: basic Owner: admin

Label: 859ba9477553ccad1bba34c555ab6a1b

Date Added: 2016-05-18 10:30:49 (UTC)

File Type: PE32:win32:gui File Size: PE32:win32:gui

MD5: 859ba9477553ccad1bba34c555ab6a1b

SHA256: 339ff6766efd4c5f26a8c0c9413b68ae664bb5eb8dfa403bec5df2909cbb73a1

Description: None

Pattern Matching Results

6 Modifies registry autorun entries

- Writes to memory of system processes
- 6 Writes to system32 folder
- 2 PE: Nonstandard section
- 5 Abnormal sleep detected
- 5 Installs service
- 3 HTTP connection response code 200 (success)
- 6 Changes Winsock providers
- 10 Creates malicious events: ZeroAccess [Rootkit]
- 4 Terminates process under Windows subfolder
- 4 Reads process memory
- 5 PE: Contains compressed section
- 3 Long sleep detected
- 7 Injects thread into Windows process

Static Events

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

Process/Thread Events

Creates process: C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe

 $["C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"]$

Creates process: C:\Windows\system32\cmd.exe ["C:\Windows\system32\cmd.exe"]
Creates process: C:\Windows\system32\rund1132.exe [C:\Windows\system32\rund1132.exe

bfe.dll,BfeOnServiceStartTypeChange]

Reads from process: PID:2712 C:\Windows\System32\calc.exe
Writes to process: PID:1096 C:\Windows\explorer.exe
Writes to process: PID:436 C:\Windows\System32\services.exe
Writes to process: PID:2660 C:\Windows\System32\cmd.exe

Terminates process: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

Terminates process: C:\Windows\System32\cmd.exe
Terminates process: C:\Windows\System32\rund1132.exe
Creates remote thread: C:\Windows\explorer.exe
Creates remote thread: C:\Windows\System32\services.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}

Creates event: \BaseNamedObjects\ConsoleEvent-0x00000A6C

File System Events

Creates: C:\\$Recycle.Bin\

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002
Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\L

Creates: C:\\$Recycle.Bin\\$-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\U

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\@

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

```
C:\$Recycle.Bin\S-1-5-18
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d
 Creates:
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\L
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
 Creates:
                         C:GAC MSIL
 Creates:
 Creates:
                         C:GAC
                         C:\Windows\assembly\GAC\Desktop.ini
 Creates:
 Creates:
                         C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
 Opens:
                         C:\Windows\Prefetch\859BA9477553CCAD1BBA34C555AB6-401FB0A4.pf
 Opens:
                         C:\Windows\System32
                         C:\windows\temp\atl.dll
 Opens:
 Opens:
                         C:\Windows\System32\atl.dll
                         C:\Windows\System32\imm32.dll
 Opens:
 Opens:
                         C:\Windows\system32\djusifdsjufkjldsdljkfh
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\System32\sechost.dll
 Opens:
                         C:\windows\temp\Cabinet.dll
 Opens:
                         C:\Windows\System32\cabinet.dll
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
                         C:\Windows\System32\rsaenh.dll
 Opens:
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
                         C:\Windows
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
                         C:\Windows\MSWSOCK.dll
 Opens:
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
 Opens:
                         C:\Windows\assembly
                         C:\Windows\assembly\GAC\Desktop.ini
 Opens:
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
 Opens:
                         C:\Windows\System32\cmd.exe
 Opens:
                         C:\Windows\System32\apphelp.dll
 Opens:
                         C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
 Opens:
                         C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
 Opens:
 Opens:
                         C:\Program Files
                         C:\Program Files\Adobe
 Opens:
 Opens:
                         C:\Program Files\Adobe\Reader 9.0
 Opens:
                         C:\Program Files\Adobe\Reader 9.0\Reader
 Opens:
                         C:\Windows\Branding
 Opens:
                         C:\Windows\Branding\Basebrd
 Opens:
                         C:\Windows\Branding\Basebrd\en-US
                         C:\Windows\Globalization
 Opens:
 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
                         C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
 Opens:
 Opens:
                         C:\Windows\Temp
 Opens:
                         C:\Windows\System32\rundll32.exe
                         C:\Windows\AppPatch\sysmain.sdb
 Opens:
 Opens:
                         C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
 Opens:
                         C:\Windows\AppPatch\AcLayers.dll
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
                         C:\Windows\System32\userenv.dll
                         C:\Windows\System32\profapi.dll
 Opens:
 Opens:
                         C:\Windows\System32\winspool.drv
 Opens:
                         C:\Windows\System32\mpr.dll
 Opens:
                         C:\Windows\System32\en-US\rundll32.exe.mui
 Opens:
                         C:\Windows\System32\BFE.DLL
 Opens:
                         C:\Windows\system32\bfe.dll.manifest
                         C:\Windows\system32\bfe.dll.123.Manifest
 Opens:
 Opens:
                         C:\Windows\system32\bfe.dll.124.Manifest
```

1002\\$b136cea6dd8900e373425c26f869789d\n

Opens: C:\Windows\system32\bfe.dll.2.Manifest

Opens: C:\Windows\System32\authz.dll
Opens: C:\Windows\System32\slc.dll

Opens: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\@

Opens: C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad

Opens: C:\Windows\System32\calc.exe

Opens: C:\

Writes to: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\@

Writes to: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\n

Writes to: C:\\$Recycle.Bin\S-1-5-18\\$b136cea6dd8900e373425c26f869789d\@ Writes to: C:\\$Recycle.Bin\S-1-5-18\\$b136cea6dd8900e373425c26f869789d\n

Writes to: C:\Windows\assembly\GAC\Desktop.ini

Writes to: C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad

Reads from: C:\Windows\Prefetch\CMD.EXE-4A81B364.pf

Reads from: C:\\$Recycle.Bin\S-1-5-18\\$b136cea6dd8900e373425c26f869789d\@

Reads from: C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad

Deletes: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

Network Events

DNS query: promos.fling.com DNS response: promos.fling.com \Rightarrow 208.91.207.58 Connects to: 208.91.207.58:80 Connects to: 213, 108, 252, 185:80 Sends data to: 8.8.8.8:53 Sends data to: promos.fling.com:80 (208.91.207.58) 213.108.252.185:80 Sends data to: Sends data to: 83.133.123.20:53 Sends data to: 37.112.0.251:16471 Sends data to: 68.104.123.244:16471 Sends data to: 99.225.75.244:16471 Sends data to: 94.240.212.241:16471 Sends data to: 111.65.195.241:16471 Sends data to: 184.66.166.241:16471 Sends data to: 74.129.114.241:16471 70.176.247.237:16471 Sends data to: Sends data to: 125.4.212.237:16471 Sends data to: 94.24.192.232:16471 Sends data to: 182.1.253.230:16471 Sends data to: 87.3.88.229:16471 Sends data to: 210.2.239.226:16471 Sends data to: 71.62.37.224:16471 Sends data to: 66.158.225.2:16471 Sends data to: 69.242.115.222:16471 Sends data to: 178.48.109.222:16471 Sends data to: 83.14.18.222:16471 Sends data to: 90.229.137.221:16471 Sends data to: 219.173.240.2:16471 Sends data to: 115.38.18.4:16471 Sends data to: 72.48.52.8:16471 Sends data to: 68.148.21.218:16471 Sends data to: 46.237.125.216:16471 Sends data to: 98.220.121.216:16471 Sends data to: 89.214.82.216:16471 Sends data to: 85.230.116.8:16471 Sends data to: 173.19.154.215:16471 Sends data to: 206.53.110.9:16471 142.167.122.9:16471 Sends data to: Sends data to: 89.132.206.9:16471 Sends data to: 75.131.172.213:16471 Sends data to: 78.23.0.213:16471 Sends data to: 186.10.14.10:16471 Sends data to: 76.123.75.212:16471 113.211.35.11:16471 Sends data to: Sends data to: 122.31.235.211:16471 Sends data to: 46.128.24.13:16471 114.74.200.13:16471 Sends data to: 87.1.83.15:16471 Sends data to: Sends data to: 138.124.19.16:16471 121.84.80.16:16471 Sends data to: 76.126.235.205:16471 Sends data to: Sends data to: 69.143.155.205:16471 151.33.20.205:16471 Sends data to: 93.171.119.17:16471 Sends data to: Sends data to: 89.181.132.204:16471 Receives data from: Receives data from: promos.fling.com:80 (208.91.207.58) 213.108.252.185:80 Receives data from:

Creates key: HKCU\software\classes\clsid

HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9} Creates key:

Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-

409d6c4515e9}\inprocserver32

Deletes value: HKLM\software\microsoft\windows\currentversion\run\windows defenderl

Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\terminal server HKLM\system\currentcontrolset\control\safeboot\option Opens key: Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key:

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 kev: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside Opens key: Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens kev: 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\system\currentcontrolset\control\nls\customlocale HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics

Opens key: HKLM\software\microsoft\sqmclient\windows

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key:

HKLM\software\policies\microsoft\sqmclient\windows

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2f2e863f

Opens kev:

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 kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000012 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000016 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000017 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000018 Opens kev:

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:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
   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\0000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006
                                              HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
   Opens key:
                                              HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
   Opens key:
                                              HKLM\system\currentcontrolset\services\psched\parameters\winsock
                                              HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens kev:
   Opens key:
                                              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
   Opens key:
                                              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
                                              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ base
   Opens kev:
cryptographic provider v1.0
   Opens key:
                                              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
                                              HKLM\system\currentcontrolset\control\lsa
   Opens key:
   Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                              HKLM\software\policies\microsoft\cryptography
   Opens kev:
   Opens key:
                                              HKLM\software\microsoft\cryptography
   Opens key:
                                              HKLM\software\microsoft\cryptography\offload
                                              {\tt HKLM \coftware \mbox{\tt microsoft \cryptography \deshashsession} keybackward}
   Opens key:
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
   Opens kev:
9a6f-135d9c6622cc}
   Opens key:
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ shells ervice objects \ `\{f56f6fdd-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4618-aa9d-4
a949-c1b91af43b1a}
                                              \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ windows \+ current \+ version \+ v
   Opens key:
   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\control\sqmservicelist
                                              HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
   Opens key:
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
                                              HKLM\system\currentcontrolset\control\session manager\appcertdlls
   Opens key:
   Opens key:
                                              HKLM\system\currentcontrolset\control\session manager\appcompatibility
   Opens key:
                                              HKLM\software\policies\microsoft\windows\appcompat
   Opens key:
                                              HKCU\software\microsoft\windows nt\currentversion
   Opens key:
                                              \label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current version\app compatflags\layers} \\
   Opens kev:
                                              HKLM\software\microsoft\windows nt\currentversion\appcompatflags
   Opens key:
                                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\profilelist
   Opens key:
                                              \label{lem:hklm} \verb+Kklm \system \current control \session manager \verb+ environment+ \\
   Opens key:
                                              HKLM\software\microsoft\windows\currentversion
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
   Opens key:
                                              HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
                                              HKLM\system\currentcontrolset\control\cmf\config
   Opens key:
   Opens key:
                                              HKU\.default\environment
   Opens key:
                                              HKU\.default\volatile environment
                                              HKU\.default\volatile environment\0
   Opens key:
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
   Opens key:
                                              HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
                                              HKLM\software\microsoft\windows
   Opens kev:
\verb|nt\currentversion\appcompatflags\custom\rundll 32.exe|
                                              HKU\.default\control
   Opens key:
panel\desktop\muicached\machinelanguageconfiguration
   Opens key:
                                              HKU\.default\software\policies\microsoft\control panel\desktop
   Opens key:
                                              HKU\.default\control panel\desktop\languageconfiguration
```

Opens key: HKU\.default\control panel\desktop
Opens key: HKU\.default\control panel\desktop\muicached

```
HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:
```

 $\label{lem:hkuldefault} $$HKU\.default\software\mbox{\sc microsoft\windows nt\currentversion\app}$$$ Opens key:

HKLM\software\microsoft\ole Opens kev:

Opens key: HKLM\software\microsoft\ole\tracing

Opens kev: HKLM\software\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder

HKLM\system\currentcontrolset\services\bfe Opens key:

Opens key: HKLM\system\currentcontrolset\services\aelookupsvc

Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0 Opens key: Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\alg

Opens key: HKLM\system\currentcontrolset\services\alg\triggerinfo

HKLM\system\currentcontrolset\services\appidsvc Opens key:

Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1 Opens kev:

Opens key: HKLM\system\currentcontrolset\services\appinfo

Opens key: HKLM\system\currentcontrolset\services\appinfo\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\appmgmt

Opens key: HKLM\system\currentcontrolset\services\appmgmt\triggerinfo HKLM\system\currentcontrolset\services\audioendpointbuilder Opens key:

HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo Opens kev:

Opens key: HKLM\system\currentcontrolset\services\audiosrv

Opens key: HKLM\system\currentcontrolset\services\audiosrv\triggerinfo

Opens key: $HKLM \verb|\system| current control set \verb|\services| axinstsv$

Opens key: HKLM\system\currentcontrolset\services\axinstsv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\bdesvc HKLM\system\currentcontrolset\services\bdesvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0

Opens key: Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1 Opens key: HKLM\system\currentcontrolset\services\bfe\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\bits

Opens key: HKLM\system\currentcontrolset\services\bits\triggerinfo

HKLM\system\currentcontrolset\services\browser Opens key:

Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\0 HKLM\system\currentcontrolset\services\browser\triggerinfo\1 Opens key: Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\2

Opens key: HKLM\system\currentcontrolset\services\bthserv

HKLM\system\currentcontrolset\services\bthserv\triggerinfo Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1 HKLM\system\currentcontrolset\services\certpropsvc Opens key:

Opens key: HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32

Opens key:

HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32\triggerinfo

HKLM\system\currentcontrolset\services\comsysapp Opens kev:

HKLM\system\currentcontrolset\services\comsysapp\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\cryptsvc Opens key: HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\cscservice

Opens key: HKLM\system\currentcontrolset\services\cscservice\triggerinfo

Opens kev: HKLM\system\currentcontrolset\services\dcomlaunch

Opens key: HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\defragsvc

HKLM\system\currentcontrolset\services\defragsvc\triggerinfo Opens key:

HKLM\system\currentcontrolset\services\dhcp Opens key:

Opens key: HKLM\system\currentcontrolset\services\dhcp\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\dnscache

HKLM\system\currentcontrolset\services\dnscache\triggerinfo Opens key: Opens key: $HKLM \verb|\system| current controlset \verb|\services| dnscache \verb|\triggerinfo|| 0$ Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1

HKLM\system\currentcontrolset\services\dot3svc Opens key:

Opens key: HKLM\system\currentcontrolset\services\dot3svc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\dps

Opens key: HKLM\system\currentcontrolset\services\dps\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\eaphost

Opens key: HKLM\system\currentcontrolset\services\eaphost\triggerinfo

 ${\it HKLM} \verb|\system| current control set \verb|\services| efs$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\ehrecvr

HKLM\system\currentcontrolset\services\ehrecvr\triggerinfo Opens kev:

 ${\it HKLM \ } system \ `current control set \ `services \ `eh sched'$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\ehsched\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\eventlog

HKLM\system\currentcontrolset\services\eventlog\triggerinfo Opens key:

Opens key: HKLM\system\currentcontrolset\services\eventsystem

Opens kev: HKLM\system\currentcontrolset\services\eventsystem\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\fax

HKLM\system\currentcontrolset\services\fax\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\fdphost Opens kev: HKLM\system\currentcontrolset\services\fdrespub Opens key: Opens kev: HKLM\system\currentcontrolset\services\fdrespub\triggerinfo Opens key: ${\it HKLM \ } system \ `current control set \ `services \ 'font cache$ HKLM\system\currentcontrolset\services\fontcache\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0 Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo HKLM\system\currentcontrolset\services\gpsvc Opens key: Opens key: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\hidserv Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0 Opens key: Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1 HKLM\system\currentcontrolset\services\hkmsvc Opens key: HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\homegrouplistener Opens key: HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo Opens key: ${\tt HKLM \ } system \verb| current control set \verb| services \verb| homegroupprovider \\$ Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo HKLM\system\currentcontrolset\services\idsvc Opens key: HKLM\system\currentcontrolset\services\idsvc\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\ikeext Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1 Opens key: HKLM\system\currentcontrolset\services\ipbusenum Opens key: HKLM\system\currentcontrolset\services\ipbusenum\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ivmservice Opens key: HKLM\system\currentcontrolset\services\keyiso Opens key: HKLM\system\currentcontrolset\services\keyiso\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ktmrm Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo $HKLM \verb|\system| current control set \verb|\services| ktmrm \verb|\triggerinfo|| 0$ Opens key: Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1 Opens key: HKLM\system\currentcontrolset\services\lanmanserver HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo HKLM\system\currentcontrolset\services\lltdsvc Opens key: Opens key: HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\lmhosts HKLM\system\currentcontrolset\services\lmhosts\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1 Opens key: Opens key: HKLM\system\currentcontrolset\services\mcx2svc HKLM\system\currentcontrolset\services\mcx2svc\triggerinfo Opens kev: ${\it HKLM} \verb|\system| current control set \verb|\services| mmcss$ Opens key: Opens key: HKLM\system\currentcontrolset\services\mmcss\triggerinfo Opens key: HKLM\system\currentcontrolset\services\msdtc Opens key: HKLM\system\currentcontrolset\services\msdtc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\msiscsi Opens kev: HKLM\system\currentcontrolset\services\msiscsi\triggerinfo Opens key: HKLM\system\currentcontrolset\services\msiserver Opens key: HKLM\system\currentcontrolset\services\msiserver\triggerinfo Opens key: HKLM\system\currentcontrolset\services\napagent HKLM\system\currentcontrolset\services\napagent\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\netlogon Opens key: HKLM\system\currentcontrolset\services\netlogon\triggerinfo Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\ Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\ Opens key: HKLM\system\currentcontrolset\services\netman HKLM\system\currentcontrolset\services\netman\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\netprofm Opens key: HKLM\system\currentcontrolset\services\netprofm\triggerinfo Opens key: ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash nett cpports haring}$ Opens key: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ nettcpport sharing \verb|\ trigger info$ Opens key: HKLM\system\currentcontrolset\services\nlasvc ${\tt HKLM} \ system \verb|\currentcontrolset\ services\ nlasvc\ trigger info}$ Opens key: Opens key: HKLM\system\currentcontrolset\services\nsi Opens key: HKLM\system\currentcontrolset\services\nsi\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ose Opens key: HKLM\system\currentcontrolset\services\ose\triggerinfo HKLM\system\currentcontrolset\services\p2pimsvc Opens kev:

Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2psvc
Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc

Opens key: HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\pla

Opens key: HKLM\system\currentcontrolset\services\pla\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\plugplay

Opens key: HKLM\system\currentcontrolset\services\plugplay\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\pnrpsvc

Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\policyagent

Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\power

Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\profsvc

Opens key: HKLM\system\currentcontrolset\services\profsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\protectedstorage

Opens key: HKLM\system\currentcontrolset\services\protectedstorage\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\qwave

Opens key: HKLM\system\currentcontrolset\services\qwave\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\rasauto

Opens key: HKLM\system\currentcontrolset\services\rasauto\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\rasman

Opens key: HKLM\system\currentcontrolset\services\rasman\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteaccess

Opens key: HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\remoteregistry

Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\rpceptmapper

Opens key: HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\rpclocator

Opens key: HKLM\system\currentcontrolset\services\rpclocator\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\rpcss

Opens key: HKLM\system\currentcontrolset\services\rpcss\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\samss

Opens key: HKLM\system\currentcontrolset\services\samss\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\sams\tr

Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\schedule

Opens key: HKLM\system\currentcontrolset\services\schedule\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\scpolicysvc
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\sdrsvc

Opens key: ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash sdrsvc \backslash triggerinfo}$

Opens key: HKLM\system\currentcontrolset\services\seclogon

Opens key: HKLM\system\currentcontrolset\services\seclogon\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\sens

Opens key: HKLM\system\currentcontrolset\services\sens\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\sensrsvc

Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\sessionenv

Opens key: HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\snmptrap

Opens key: HKLM\system\currentcontrolset\services\snmptrap\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\spooler

Opens key: HKLM\system\currentcontrolset\services\spooler\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\sppsvc

Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\sppuinotify

Opens key: HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\ssdpsrv

Opens key: ${\tt HKLM \ } {\tt System \ } {\tt Current control set \ } {\tt Services \ } {\tt Ssdpsrv \ } {\tt trigger info}$

Opens key: HKLM\system\currentcontrolset\services\sstpsvc

Opens key: HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\stisvc

Opens key: ${\tt HKLM \setminus system \setminus current control set \setminus services \setminus stisvc \setminus triggerinfo}$

Opens key: HKLM\system\currentcontrolset\services\storsvc

Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\swprv

Opens key: ${\tt HKLM \ } {\tt System \ } {\tt current controlset \ } {\tt swprv \ } {\tt triggerinfo}$

Opens key: HKLM\system\currentcontrolset\services\sysmain

Opens key: HKLM\system\currentcontrolset\services\sysmain\triggerinfo Opens key: HKLM\system\currentcontrolset\services\tabletinputservice

Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\tapisrv

HKLM\system\currentcontrolset\services\tapisrv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\tbs Opens key: ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash tbs \backslash trigger in fo}$ Opens kev: Opens key: HKLM\system\currentcontrolset\services\termservice Opens kev: HKLM\system\currentcontrolset\services\termservice\triggerinfo Opens key: ${\it HKLM \ } system \ `current control set \ `services \ 'themes$ HKLM\system\currentcontrolset\services\themes\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\threadorder HKLM\system\currentcontrolset\services\threadorder\triggerinfo Opens key: HKLM\system\currentcontrolset\services\tlntsvr Opens key: HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\trkwks Opens key: HKLM\system\currentcontrolset\services\trkwks\triggerinfo HKLM\system\currentcontrolset\services\trustedinstaller Opens key: HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ui0detect Opens key: Opens key: HKLM\system\currentcontrolset\services\ui0detect\triggerinfo Opens key: HKLM\system\currentcontrolset\services\umrdpservice Opens key: HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo HKLM\system\currentcontrolset\services\upnphost Opens key: Opens key: HKLM\system\currentcontrolset\services\upnphost\triggerinfo HKLM\system\currentcontrolset\services\uxsms Opens key: HKLM\system\currentcontrolset\services\uxsms\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\vaultsvc Opens key: HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\vds Opens key: HKLM\system\currentcontrolset\services\vds\triggerinfo Opens key: HKLM\system\currentcontrolset\services\vss Opens key: HKLM\system\currentcontrolset\services\vss\triggerinfo Opens key: HKLM\system\currentcontrolset\services\w32time Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1 Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\2 Opens key: HKLM\system\currentcontrolset\services\wbengine Opens key: HKLM\system\currentcontrolset\services\wbengine\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wbiosrvc Opens key: HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wcncsvc Opens key: HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo ${\tt HKLM \ } system \verb| current control set \verb| services \verb| wcspluginservice| \\$ Opens key: Opens key: HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wdiservicehost HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\wdisystemhost Opens key: HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo ${\it HKLM} \verb|\system| current control set \verb|\services| we belient \\$ Opens key: Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0 Opens key: Opens key: HKLM\system\currentcontrolset\services\wecsvc Opens key: HKLM\system\currentcontrolset\services\wecsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wercplsupport Opens key: HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo Opens kev: HKLM\system\currentcontrolset\services\wersvc Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1 HKLM\system\currentcontrolset\services\winhttpautoproxysvc Opens key: Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\winmgmt Opens key: HKLM\system\currentcontrolset\services\winmgmt\triggerinfo Opens key: HKLM\system\currentcontrolset\services\winrm Opens key: HKLM\system\currentcontrolset\services\winrm\triggerinfo HKLM\system\currentcontrolset\services\wlansvc Opens key: Opens key: HKLM\system\currentcontrolset\services\wlansvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wmiapsrv HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo ${\it HKLM} \verb|\system| current control set \verb|\services| \verb|\wpcsvc| \\$ Opens key: Opens key: HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wpdbusenum ${\it HKLM \ } system \ {\it current controlset \ } wices \ {\it wpdbusenum \ } trigger in fo$ Opens key: Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0 HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1 Opens kev: $HKLM \verb|\system| current controlset \verb|\services| wpdbusenum \verb|\triggerinfo|| 2$ Opens key: Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3 Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4

Opens key: HKLM\system\currentcontrolset\services\wsearch Opens key: HKLM\system\currentcontrolset\services\wsearch\triggerinfo HKLM\system\currentcontrolset\services\wuauserv Opens kev:

Opens key: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\wudfsvc Opens key: HKLM\svstem\currentcontrolset\services\wudfsvc\triggerinfo Opens kev: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1 Opens key: Opens key: HKLM\system\currentcontrolset\services\wwansvc Opens key: HKLM\system\currentcontrolset\services\wwansvc\triggerinfo HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b} Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b} Opens key: Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid Opens key: Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32 HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32 Opens kev: Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32 HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32 Opens key: Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler Opens kev: Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8} Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8} Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708a0b2badd77c8}\treatas Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-Opens kev: a0b2badd77c8}\progid Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708a0b2badd77c8}\inprocserver32 Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32 HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-Opens key: a0b2badd77c8}\inprochandler32 HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler32 Opens kev: Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708a0b2badd77c8}\inprochandler $HKCR \ clsid \ \{a2a9545d-a0c2-42b4-9708-a0b2badd77c8\} \ \ in prochandler$ Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{90aa3a4e-1cba-4233-b8bb-535773d48449\}$ Opens key: Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449} Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32 HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32 Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-Opens key: 535773d48449}\inprochandler32 $HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\tinprochandler 32abbb-535773d48449\}\tinprochandler 32abbb-535773d48449$ Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-Opens key: 535773d48449}\inprochandler Opens key: HKCU\software\classes\applications\calc.exe Opens key: HKCR\applications\calc.exe Opens key: Opens key: HKLM\software\microsoft\ctf\knownclasses Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c} Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c} Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid $HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid$ Opens key: Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32 HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32 Opens key: Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler $HKCR \clsid \dd313e04-feff-11d1-8ecd-0000f87a470c \hipprochandler$ Opens key:

Queries value:

manager[cwdillegalindllsearch]

Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]$

Queries value: HKCU\control panel\desktop[preferreduilanguages]

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Oueries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Oueries value: HKLM\system\currentcontrol\set\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[859ba9477553ccad1bba34c555ab6a1b]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\system\currentcontrol\sct\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrol\set\control\nls\extendedlocale[en-us]

Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [winsock_registry_version]$

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]

Queries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog9[serial_access_num]$

Queries value:

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\000000000003[packedcatalogitem]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000004 \ [packed catalog item] \\ Oueries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000006[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000009 \ [packed catalog item] \ Queries \ value:$

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\000000000013[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000015 \ [packed catalog item] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]

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]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000001 \ [version] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo]

- Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Oueries 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]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \catalog_entries \namespace_catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \cat$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000005 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000006 [library path] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000006 [supported name space] \\ Queries \ value:$

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 00000000000006[enabled]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog\_entries \ (00000000006[storesserviceclass info]) \ (catalog\_entries) \ 
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  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]
                                    HKLM\system\currentcontrolset\services\winsock\setup
  Oueries value:
migration\providers\psched[winsock 2.0 provider id]
                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
  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:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [helperdllname]
                                     HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
  Queries value:
cryptographic provider v1.0[type]
                                    HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
  Queries value:
cryptographic provider v1.0[image path]
  Queries value:
                                     HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                     HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:
                                     HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Oueries value:
  Oueries value:
                                    HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Oueries value:
                                     HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                     HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Oueries value:
options\dllnxoptions[usefilter]
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Oueries value:
options\dllnxoptions[n]
  Queries value:
                                    HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\svstem\currentcontrolset\computername\activecomputername[computername]
  Queries value:
                                     HKLM\system\setup[oobeinprogress]
  Oueries value:
                                     HKLM\system\setup[systemsetupinprogress]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
                                     HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion[programfilesdir]
                                     HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
  Oueries value:
                                     HKLM \setminus software \setminus microsoft \setminus windows \setminus current version [common files dir (x86)] \\
  Queries value:
                                     HKLM \setminus software \setminus microsoft \setminus windows \setminus current version [programw6432 dir] \\
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion[commonw6432dir1
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
18[profileimagepath]
  Queries value:
                                     HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
                                     HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Queries value:
                                     HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
  Oueries value:
                                     HKU\.default\control panel\desktop[preferreduilanguages]
  Oueries value:
                                     HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
                                     HKLM\software\microsoft\windows
  Oueries value:
```

nt\currentversion\compatibility32[rundl132]

Oueries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKLM\system\currentcontrolset\services\bfe[imagepath] Queries value: HKLM\system\currentcontrolset\services\bfe[type] Oueries value: HKLM\svstem\currentcontrolset\services\bfe[start] Queries value: HKLM\system\currentcontrolset\services\bfe[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\bfe[tag] Oueries value: HKLM\system\currentcontrolset\services\bfe[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\bfe[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\bfe[group] Oueries value: HKLM\system\currentcontrolset\services\bfe[objectname] Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action] Oueries value: Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0] Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action] Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type] HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid] Queries value: Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0] Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2] HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2] Queries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0] HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0] Queries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1] Oueries value: $HKLM \ system \ current control set \ services \ browser \ trigger in fo \ 1 \ [data1]$ HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2] Queries value: Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1ſdata21 Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3] HKLM\system\currentcontrolset\services\browser[imagepath] Oueries value: Queries value: HKLM\system\currentcontrolset\services\browser[type] Oueries value: HKLM\system\currentcontrolset\services\browser[start] Queries value: HKLM\system\currentcontrolset\services\browser[errorcontrol] Oueries value: HKLM\svstem\currentcontrolset\services\browser[tag] Oueries value: HKLM\system\currentcontrolset\services\browser[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\browser[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\browser[group] Oueries value: HKLM\system\currentcontrolset\services\browser[objectname] Queries value: Oueries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action1 Oueries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type] HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0] Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache[imagepath] Oueries value: HKLM\system\currentcontrolset\services\dnscache[type] HKLM\system\currentcontrolset\services\dnscache[start] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache[tag] Queries value: HKLM\system\currentcontrolset\services\dnscache[dependonservice] HKLM\system\currentcontrolset\services\dnscache[dependongroup] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache[group] Oueries value: HKLM\system\currentcontrolset\services\dnscache[objectname] Oueries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid] HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0] Oueries value: Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0] Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]

HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]

Queries value:

```
Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[tag]
                          HKLM\system\currentcontrolset\services\ikeext[dependonservice]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
 Queries value:
                          HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
                          HKLM \verb|\system| current controlset \verb|\services| lmhosts \verb|\triggerinfo| 1 [data type 0]
 Queries value:
 Queries value:
                          HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \texttt{[a66e19e6]}
 Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
 Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
 Queries value:
                          Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
                         HKLM\system\currentcontrolset\services\policyagent[imagepath]
 Queries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[type]
                          HKLM\system\currentcontrolset\services\policyagent[start]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\policyagent[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\policyagent[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\policyagent[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent[objectname]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
 Oueries value:
                          HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
 Queries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
 Queries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus table tinput service \setminus trigger in fo \setminus 0 \ [guid]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype3]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype4]
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
```

HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]

HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]

Oueries value:

Queries value:

```
Oueries value:
                        HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
                        HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
 Oueries value:
 Oueries value:
                        HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
 Queries value:
                        HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
 Oueries value:
                        HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
 Queries value:
                        HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
 Oueries value:
                        HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[type]
 Oueries value:
                        HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
                        HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]
 Oueries value:
 Queries value:
                        HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
 Oueries value:
                        HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
 Oueries value:
                        HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
 Queries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
 Queries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
 Oueries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
 Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
 Queries value:
 Queries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
 Queries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
 Queries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
 Queries value:
 Queries value:
                        HKLM \setminus system \setminus current control set \setminus services \setminus wpdbusenum \setminus triggerinfo \setminus 2 [guid]
 Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
 Queries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
 Oueries value:
                        HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
                        HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
 Oueries value:
                        HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
 Queries value:
 Queries value:
                        HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
 Oueries value:
                        HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
                        HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
 Queries value:
 Queries value:
                        HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
                        HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
 Oueries value:
                        HKCR\clsid\{660b90c8-73a9-4b58-8cae-
 Queries value:
355b7f55341b}\inprocserver32[inprocserver32]
                        Queries value:
                        HKCR\clsid\{660b90c8-73a9-4b58-8cae-
 Oueries value:
355b7f55341b}\inprocserver32[threadingmodel]
                        HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
 Queries value:
 Queries value:
                        HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
 Queries value:
                        HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
                        HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
 Oueries value:
a0b2badd77c8}\inprocserver32[threadingmodel]
                        HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
 Queries value:
                        HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
 Queries value:
535773d48449}\inprocserver32[inprocserver32]
 Queries value:
                        HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[]
                        HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
 Oueries value:
535773d48449}\inprocserver32[threadingmodel]
                        HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[]
 Oueries value:
                        HKCR\clsid\{dd313e04-feff-11d1-8ecd-
 Queries value:
0000f87a470c}\inprocserver32[inprocserver32]
 Queries value:
                        HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
                        HKCR\clsid\{dd313e04-feff-11d1-8ecd-
 Queries value:
0000f87a470c}\inprocserver32[threadingmodel]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
 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[]
                        HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
 Value changes:
 Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000018 \ [packed catalog item]
 Value changes:
Value changes:
Value changes:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 000000000014 \ [packed catalog item]$

Value changes:

Value changes:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem] Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 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\0000000000010[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\00000000007[packedcatalogitem] Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem] Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[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\00000000001[packedcatalogitem] Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
 Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]

Value changes: HKLM\system\currentcontrolset\services\browser[start]
Value changes: HKLM\system\currentcontrolset\services\policyagent[start]

Value changes:

9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]

Value changes:

HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-

9926f41749ea}\count[hrzr_pgyfrffvba]