Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3331, Task ID: 834

Task ID: 834 Risk Level: 10

Date Processed: 2016-05-18 10:44:09 (UTC)

Processing Time: 80.5 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"

Sample ID: Type: basic admin Owner:

1be5bc13fd1cf615a95feec0c5b7fd13 Label: 2016-05-18 10:30:52 (UTC)

Date Added: PE32:win32:gui

File Type: File Size: 201728 bytes

1be5bc13fd1cf615a95feec0c5b7fd13 MD5:

10e3f54492e5cdcdf2c1ae6d097aafdea9474ff77bf6ccb5a9c762ccb6e4a347 SHA256:

Description: None

Pattern Matching Results

Writes to memory of system processes

- Modifies registry autorun entries
- 6 Writes to system32 folder
- 5 Abnormal sleep detected
- 5 Installs service
- 10 Creates malicious events: ZeroAccess [Rootkit]
- 6 Changes Winsock providers
- 3 Connects to local host
- 4 Terminates process under Windows subfolder
- 4 Reads process memory
- 3 Long sleep detected
- 7 Injects thread into Windows process

Process/Thread Events

Creates process: C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe

["C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"]

C:\Windows\SysWOW64\cmd.exe ["C:\Windows\system32\cmd.exe"] Creates process:

PID:2620 C:\Windows\SysWOW64\calc.exe Reads from process: Writes to process: PID:296 C:\Windows\explorer.exe Writes to process: PID:444 C:\Windows\System32\services.exe PID:2476 C:\Windows\SysWOW64\cmd.exe Writes to process:

Terminates process: C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe

C:\Windows\SysWOW64\cmd.exe Terminates process: Creates remote thread: C:\Windows\explorer.exe Creates remote thread: C:\Windows\System32\services.exe C:\Windows\System32\sppsvc.exe Creates remote thread:

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex \BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1} Creates event: Creates event: Creates events \BaseNamedObjects\SvcctrlStartEvent_A3752DX

\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77} Creates event:

Creates event: \BaseNamedObjects\ConsoleEvent-0x00000000000009D8

File System Events

Creates C:\\$Recycle.Bin\ Creates

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-Creates

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2 Creates

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\L

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-Creates

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\U C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-Creates

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\@

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\n

Creates: C:\\$Recycle.Bin\S-1-5-18

Creates: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2 C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\L Creates: Creates: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\U C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\@ Creates: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\n Creates:

Creates: C:GAC MSIL Creates: C:GAC

```
C:GAC_32
 Creates:
                         C:GAC 64
 Creates:
                         C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
 Creates:
                         C:\Windows\assembly\GAC_64\Desktop.ini
 Creates:
 Creates:
                         C:\Windows\assembly\GAC_32\Desktop.ini
 Opens:
                         C:\Windows\Prefetch\1BE5BC13FD1CF615A95FEEC0C5B7F-CFDFB467.pf
 Opens:
                         C:\Windows
                         C:\Windows\System32\wow64.dll
 Opens:
 Opens:
                         C:\Windows\System32\wow64win.dll
                         C:\Windows\System32\wow64cpu.dll
 Opens:
 Opens:
                         C:\Windows\system32\wow64log.dll
 Opens:
                         C:\Windows\SysWOW64
 Opens:
                         C:\Windows\SysWOW64\sechost.dll
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\Windows\SysWOW64\includeincludeincludeincludeinclude\
 Opens:
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\windows\temp\Cabinet.dll
 Opens:
                         C:\Windows\SysWOW64\cabinet.dll
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\System32\Actioncenter.dll.3.Manifest
 Opens:
                         C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
                         C:\windows\temp\CRYPTSP.dll
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
                         C:\Windows\MSWSOCK.dll
 Opens:
 Opens:
                         C:\Windows\System32\mswsock.dll
                         C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
 Opens:
 Opens:
                         C:\Windows\assembly
 Opens:
                         C:\Windows\assembly\GAC_32\Desktop.ini
 Opens:
                         C:\Windows\assembly\GAC_64\Desktop.ini
 Opens:
                         C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
                         {\tt C:\Windows\SysWOW64\cmd.exe}
 Opens:
 Opens:
                         C:\Windows\SysWOW64\apphelp.dll
 Opens:
                         C:\Windows\AppPatch\sysmain.sdb
 Opens:
                         C:\
 Opens:
                         C:\Windows\SysWOW64\ui\SwDRM.dll
 Opens:
                         C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
                         C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
 Opens:
 Opens:
                         C:\Windows\SysWOW64\winbrand.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\cmd.exe.mui
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
 Opens:
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
                         C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
 Opens:
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Windows\SysWOW64\calc.exe
 Writes to:
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
                         C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
 Writes to:
                         C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
 Writes to:
 Writes to:
                         C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
 Writes to:
                         C:\Windows\assembly\GAC_64\Desktop.ini
 Writes to:
                         C:\Windows\assembly\GAC_32\Desktop.ini
 Reads from:
                         C:\Windows\SysWOW64\cmd.exe
                         \label{lem:c:secycle.Bin\s-1-5-18} $$aaa1415b79b8dbbd8bd16c842c1858a2\\ @
 Reads from:
 Reads from:
                         C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
                         C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Network Events
```

DNS query:	j.maxmind.com
DNS response:	$j.maxmind.com \Rightarrow 127.0.0.1$
Connects to:	127.0.0.1:80
Sends data to:	8.8.8:53
Sends data to:	83.133.123.20:53
Sends data to:	206.254.253.254:16470
Sends data to:	190.254.253.254:16470
Sends data to:	180.254.253.254:16470
Sends data to:	135.254.253.254:16470
Sends data to:	115.254.253.254:16470
Sends data to:	88.254.253.254:16470
Sends data to:	87.254.253.254:16470
Sends data to:	71.254.253.254:16470
Sends data to:	243.253.253.254:16470
Sends data to:	241.253.253.254:16470
Sends data to:	240.253.253.254:16470

```
Sends data to:
                         213.253.253.254:16470
Sends data to:
                         212.253.253.254:16470
Sends data to:
                         201.253.253.254:16470
Sends data to:
                         190.253.253.254:16470
Sends data to:
                         24.125.167.254:16470
Sends data to:
                         200.85.163.252:16470
Sends data to:
                         76.123.113.252:16470
                         75.179.58.251:16470
Sends data to:
Sends data to:
                         188.24.139.250:16470
Sends data to:
                         67.169.22.247:16470
Sends data to:
                         24.91.128.246:16470
Sends data to:
                         65.190.35.245:16470
Sends data to:
                         76.29.170.239:16470
                         5.13.167.239:16470
Sends data to:
Sends data to:
                         82.131.125.232:16470
Sends data to:
                         68.37.72.231:16470
                         219.106.83.230:16470
Sends data to:
Sends data to:
                         68.61.232.228:16470
Sends data to:
                         76.107.98.5:16470
                         69.199.239.225:16470
Sends data to:
```

Receives data from: 0.0.0.0:0

Windows Registry Events

HKCU\software\microsoft\windows\currentversion\action Creates key: center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100 HKCU\software\microsoft\windows\currentversion\action Creates key: center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78} Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101 Creates key: HKCU\software\microsoft\windows\currentversion\action

 $center \verb|\providers| eventlog \verb|\{a5268b8e-7db5-465b-bab7-bdcda39a394a\}|$ HKCU\software\microsoft\windows\currentversion\action Creates key:

center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100

Creates key: HKCU\software\classes\clsid

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

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

409d6c4515e9}\inprocserver32

HKLM\software\microsoft\windows\currentversion\run[windows defender] Deletes value: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options

 $\label{lem:hklm} \verb+Kklm \+ system \+ current controls et \+ control \+ session \+ manager$ Opens key:

Opens key: HKLM\software\microsoft\wow64

HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file Opens key:

execution options

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

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ mui \+ uilanguages \+ pending delete$ Opens kev:

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

HKCU\ Opens key:

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

 ${\it HKCU \backslash control panel \backslash desktop \backslash muicached}$ Opens key:

Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side$

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKI M\

HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\diagnostics

HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\gre_initialize HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\compatibility32

Opens key:

compatibility

HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows Opens key:

HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: Opens key: HKLM\software\policies\microsoft\sqmclient\windows

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1e6c4482

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004

Opens key:

Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}

Opens key: HKLM\software\microsoft\windows\currentversion\action

 $center \verb|\providers| \{a5268b8e-7db5-465b-bab7-bdcda39a394a\}$

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\software\microsoft\windows\currentversion\action center
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

Opens key:

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic

provider v1.0 Opens key:

HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

Opens key: HKLM\system\currentcontrol\lsa

Opens key:

Opens key: HKLM\software\microsoft\cryptography

Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload

Opens key:

 $HKLM \label{lem:hardwow6432} In ode \mbox{$\mbox{$\mbox{ward$}$} icrosoft \mbox{$\mbox{$\mbox{$\mbox{$c$ryptography$} \mbox{$\mbox{$\mbox{$\mbox{$ward}$}$} icrosoft \mbox{$\mbox{}\mbox{$

Opens key:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-9a6f-135d9c6622cc\}}$

Opens key:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ shells ervice objects \ \{f56f6fdd-aa9d-4618-a949-c1b91af43b1a\}$

 $\label{lem:lem:cosoft} Opens \; key: \\ \qquad \qquad \mathsf{HKLM} \backslash \mathsf{software} \backslash \mathsf{microsoft} \backslash \mathsf{windows} \backslash \mathsf{currentversion} \backslash \mathsf{run}$

Opens key: HKLM\software\wow6432node\microsoft\rpc

 $Opens\;key: \\ \qquad \qquad \text{HKLM} \\ system \\ \text{currentcontrolset} \\ \text{control} \\ \text{computername} \\ \text{active computername} \\$

Opens key: HKLM\system\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrol\sqmservicelist

```
HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\bfe
 Opens key:
                    HKLM\system\currentcontrolset\services\aelookupsvc
                    HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo
 Opens key:
 Opens key:
                    HKLM\svstem\currentcontrolset\services\aelookupsvc\triggerinfo\0
 Opens key:
                    HKLM\system\currentcontrolset\services\alg
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\alg\triggerinfo
 Opens key:
                    HKLM\system\currentcontrolset\services\appidsvc
                    HKLM\system\currentcontrolset\services\appidsvc\triggerinfo
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0
 Opens key:
                    HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
 Opens key:
                    HKLM\system\currentcontrolset\services\appinfo
                    HKLM\system\currentcontrolset\services\appinfo\triggerinfo
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\appmgmt
 Opens key:
                    HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
                    HKLM\system\currentcontrolset\services\audioendpointbuilder
 Opens kev:
 Opens key:
                    HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
 Opens key:
                    HKLM\system\currentcontrolset\services\audiosrv
                    HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\axinstsv
 Opens key:
                    HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\00000000010
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000008
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000005
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000003
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000000
 Opens kev:
HKLM\system\currentcontrolset\services\bdesvc
 Opens kev:
                    HKLM \verb|\system| current controlset \verb|\services| bdesvc \verb|\triggerinfo| \\
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0
 Opens key:
                    HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
 Opens key:
Opens kev:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\bfe\triggerinfo
 Opens kev:
 Opens key:
Opens key:
Opens key:
                    HKLM\system\currentcontrolset\services\bits
 Opens key:
                    HKLM\system\currentcontrolset\services\bits\triggerinfo
 Opens key:
                    HKLM\system\currentcontrolset\services\browser
 Opens key:
                    HKLM\system\currentcontrolset\services\browser\triggerinfo
 Opens key:
                    HKLM\system\currentcontrolset\services\browser\triggerinfo\0
                    HKLM \verb|\software\microsoft\cryptography\defaults\provider\microsoft\ base
 Opens key:
cryptographic provider v1.0
 Opens key:
                    HKLM\system\currentcontrolset\services\browser\triggerinfo\1
                    {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash offload}
 Opens key:
 Opens key:
                    {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash deshash session key backward}
                    HKLM\system\currentcontrolset\services\browser\triggerinfo\2
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\dcomlaunch
 Opens key:
                    HKLM\system\currentcontrolset\services\rpceptmapper
 Opens key:
                    HKLM\system\currentcontrolset\services\rpcss
 Opens key:
                    HKLM\system\currentcontrolset\services\wuauserv
 Opens key:
                    HKLM\system\currentcontrolset\services\cryptsvc
 Opens kev:
                    HKLM\svstem\currentcontrolset\services\bthserv
                    HKLM\system\currentcontrolset\services\bthserv\triggerinfo
 Opens key:
 Opens key:
                    HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
 Opens key:
                    HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
 Opens key:
                    HKLM\system\currentcontrolset\services\certpropsvc
 Opens key:
                    HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
 Opens kev:
                    HKLM \setminus system \setminus current control set \setminus services \setminus clr\_optimization\_v2.0.50727\_32
 Opens key:
```

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

HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64\triggerinfo

Opens kev: 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

HKLM\software\wow6432node\policies\microsoft\windows\appcompat Opens key:

Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens kev: 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

HKLM\software\microsoft\windows Opens kev:

nt\currentversion\appcompatflags\custom\cmd.exe

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

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

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

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

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

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

Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\system\currentcontrolset\services\gpsvc Opens key: HKLM\system\currentcontrolset\services\dhcp

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

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

HKLM\svstem\currentcontrolset\services\dnscache\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1

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

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

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

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

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

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

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

Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\0 $HKLM \verb|\system| current control set \verb|\services| efs \verb|\triggerinfo| 1$ Opens key:

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

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

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

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

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

Opens key:

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

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

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

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

 ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ fdphost \verb|\ trigger info$ Opens key:

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

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

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

Opens key: HKLM\system\currentcontrolset\services\fontcache\triggerinfo Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0

HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo 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 Opens key: Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1

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

Opens key: HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\homegrouplistener

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} is $$ system \current control set \end{tabular} is $$ services \end{tabular} is $$ homegroup listener \trigger info $$ system \end{tabular} is $$ system \end{tabula$ Opens key:

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:

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

 ${\it HKLM} \verb|\system| current controlset \verb|\services| ipbus enum \\$ Opens key:

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

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

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

HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1 Opens key: Opens kev: HKLM\system\currentcontrolset\services\lanmanserver Opens key: HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo Opens kev: HKLM\system\currentcontrolset\services\lanmanworkstation Opens key: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ lanman work station \verb|\ trigger info$ HKLM\system\currentcontrolset\services\lltdsvc Opens key: HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\lmhosts Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0 Opens key: Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2 HKLM\system\currentcontrolset\services\mcx2svc Opens key: HKLM\system\currentcontrolset\services\mcx2svc\triggerinfo Opens key: HKLM\system\currentcontrolset\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 HKLM\system\currentcontrolset\services\msiscsi Opens key: Opens key: HKLM\system\currentcontrolset\services\msiscsi\triggerinfo HKLM\system\currentcontrolset\services\msiserver Opens key: HKLM\system\currentcontrolset\services\msiserver\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\napagent Opens key: HKLM\system\currentcontrolset\services\napagent\triggerinfo Opens key: HKLM\system\currentcontrolset\services\netlogon Opens key: HKLM\system\currentcontrolset\services\netlogon\triggerinfo Opens key: HKLM\system\currentcontrolset\services\netman HKLM\system\currentcontrolset\services\netman\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\netprofm Opens key: HKLM\system\currentcontrolset\services\netprofm\triggerinfo Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo Opens key: HKLM\system\currentcontrolset\services\nlasvc HKLM\system\currentcontrolset\services\nlasvc\triggerinfo 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 Opens key: HKLM\system\currentcontrolset\services\p2pimsvc $HKLM \verb|\system| current controlset \verb|\services| p2pimsvc \verb|\triggerinfo|$ Opens key: Opens key: HKLM\system\currentcontrolset\services\p2psvc Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo HKLM\system\currentcontrolset\services\pcasvc Opens key: Opens key: HKLM\system\currentcontrolset\services\pcasvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\peerdistsvc HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\perfhost Opens key: HKLM\system\currentcontrolset\services\perfhost\triggerinfo HKLM\system\currentcontrolset\services\pla Opens key: Opens key: HKLM\system\currentcontrolset\services\pla\triggerinfo Opens key: HKLM\system\currentcontrolset\services\plugplay ${\tt HKLM \ } system \verb|\ current controlset \verb|\ services \verb|\ plugplay \verb|\ triggerinfo|$ Opens key: Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg Opens kev: HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo ${\it HKLM} \verb|\system| current control set \verb|\services| pnrpsvc$ Opens key: Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\policyagent HKLM\system\currentcontrolset\services\policyagent\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1 HKLM\system\currentcontrolset\services\power Opens key: Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo Opens key: HKLM\system\currentcontrolset\services\profsvc HKLM\system\currentcontrolset\services\profsvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\protectedstorage Opens key: HKLM\system\currentcontrolset\services\protectedstorage\triggerinfo Opens key: HKLM\system\currentcontrolset\services\gwave Opens key: HKLM\system\currentcontrolset\services\qwave\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rasauto HKLM\system\currentcontrolset\services\rasauto\triggerinfo Opens key: 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

HKLM\system\currentcontrolset\services\remoteregistry Opens kev: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rpclocator HKLM\system\currentcontrolset\services\rpclocator\triggerinfo Opens key:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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: HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo

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

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

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

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

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

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: HKLM\system\currentcontrolset\services\swprv\triggerinfo

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

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

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

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

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

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

 $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ trigger in fo$ Opens key: Opens key: HKLM\system\currentcontrolset\services\termservice

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

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

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

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

 ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ thread order \verb|\ trigger info$ Opens key:

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

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

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

Opens key: HKLM\system\currentcontrolset\services\trkwks\triggerinfo Opens key: HKLM\system\currentcontrolset\services\trustedinstaller

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

Opens key: HKLM\system\currentcontrolset\services\ui0detect

Opens key: HKLM\system\currentcontrolset\services\ui0detect\triggerinfo

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

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

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

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

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

Opens key: HKLM\system\currentcontrolset\services\uxsms\triggerinfo HKLM\system\currentcontrolset\services\vaultsvc Opens key:

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

HKLM\system\currentcontrolset\services\vss\triggerinfo Opens kev: $HKLM \verb|\system| current control set \verb|\services| \verb|\w32time| \\$ Opens key:

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

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

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

```
Opens key:
                         HKLM\system\currentcontrolset\services\wbiosrvc
 Opens key:
                         HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
 Opens kev:
                         HKLM\system\currentcontrolset\services\wcncsvc
                         HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
 Opens key:
 Opens kev:
                         HKLM\system\currentcontrolset\services\wcspluginservice
 Opens key:
                         HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\wdiservicehost
 Opens key:
                         HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\wdisystemhost
 Opens key:
                         HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
                         HKLM\system\currentcontrolset\services\webclient
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
 Opens key:
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
 Opens key:
                         HKLM\system\currentcontrolset\services\wecsvc
 Opens key:
                         HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
                         HKLM\system\currentcontrolset\services\wercplsupport
 Opens kev:
 Opens key:
                         HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
 Opens key:
                         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
 Opens kev:
                         HKLM\svstem\currentcontrolset\services\winhttpautoproxvsvc
 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
 Opens key:
                         {\it HKLM} \verb|\system| current control set \verb|\services| wlansvc
 Opens key:
                         HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\wmiapsrv
 Opens key:
                         HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\wmpnetworksvc
 Opens key:
                         HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
                         {\it HKLM} \verb|\system| current control set \verb|\services| wpcsvc
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\wpdbusenum
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0
 Opens key:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
                         Opens key:
 Opens key:
                         HKLM \ system \ current controls et \ services \ wpdbusenum \ trigger in fo \ \ 3
 Opens key:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
 Opens key:
                         HKLM\system\currentcontrolset\services\wscsvc
 Opens key:
                         HKLM\system\currentcontrolset\services\wscsvc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\wsearch
                         Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
 Opens kev:
                         HKLM\svstem\currentcontrolset\services\wudfsvc
 Opens key:
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
 Opens key:
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
 Opens key:
                         HKLM\system\currentcontrolset\services\wwansvc
 Opens key:
                         HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
 Opens kev:
                         HKLM\svstem\currentcontrolset\services
 Opens key:
                         HKLM\system\currentcontrolset\services\wscsvc\parameters
                         HKLM\system\currentcontrolset\services\wscsvc\security
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows\windows error reporting\wmr
                         HKLM\software\microsoft\windows\currentversion\setup
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows\currentversion
 Opens key:
                         HKCU\control panel\international
 Opens key:
                         HKLM\system\currentcontrolset\services\crypt32
 Opens key:
                         HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash msasn1
 Opens key:
                         HKLM\system\currentcontrolset\control\idconfigdb
                         HKLM\system\currentcontrolset\control\idconfigdb\hardware profiles\0001
 Opens key:
 Opens key:
                         HKLM \verb|\system| current control \verb|\idconfigdb| current dock in fo
 Opens key:
                         HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
                         HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\treatas
                         HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\progid
                         HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\\\ \progid
 Opens key:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}
 Opens key:
                         HKCR\wow6432node\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
 Opens kev:
Opens key:
```

Opens kev:

 $\label{thm:locality} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the constraint$ $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mycomputer \setminus names pace$

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ lex plorer \ moreover \ lex plorer \ moreover \ mo$

Opens kev:

HKCU\software\microsoft\windows\currentversion\explorer\mycomputer\namespace

Opens kev:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus explorer \setminus mycomputer \setminus namespace \setminus delegate folders \setminus \{35786d3c-microsoft \setminus mycomputer \setminus namespace \setminus delegate folders \setminus \{35786d3c-microsoft \setminus mycomputer \setminus namespace \setminus delegate folders \setminus \{35786d3c-microsoft \setminus mycomputer \setminus namespace \setminus delegate folders \setminus \{35786d3c-microsoft \setminus mycomputer \setminus$

b075-49b9-88dd-029876e11c01}

Opens key: HKCU\software\classes\clsid\{26ee0668-a00a-44d7-9371-

beb064c98683}\shellfolder

Opens key: $\label{lem:hkcr} \mbox{HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder}$

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprocserver32

Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserver32

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprochandler32

Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler32

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprochandler

Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\treatas

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{9113a02d-

00a3-46b9-bc5f-9c04daddd5d7}

Opens key:

 $HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{b155bdf8-02f0-451e-9a26-ae317cfd7779\}}$

Opens key:

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ session in followy computer \ names pace$

Opens key

Opens key: HKCU\software\classes\clsid\{35786d3c-b075-49b9-88dd-

029876e11c01}\shellfolder

Opens key: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder

Opens key: HKLM\software\microsoft\windows

d6ec3f16059f

Opens key: HKLM\software\microsoft\windows

d6ec3f16059f

Opens key: HKLM\software\microsoft\windows

d6ec3f16059f

Opens key: HKLM\software\microsoft\windows

d6ec3f16059f

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\progid

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}

768597bd7223}\progid

Opens key: HKCR\wow6432node\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\progid

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

 $768597bd7223 \} \verb|\inprocserver32|$

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{26ee0668-

a00a-44d7-9371-beb064c98683}\shellfolder

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{26ee0668-

a00a-44d7-9371-beb064c98683}\shellfolder

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprochandler32

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprochandler

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler
Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}

Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{35786d3c-

b075-49b9-88dd-029876e11c01}\shellfolder

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{35786d3c-

b075-49b9-88dd-029876e11c01}\shellfolder

Opens key:

4e32-a8e8-8d23b85255bf}

Opens key: HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}

HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d} Opens key:

Opens kev:

a2dd-08002b30309d}

Opens key:

a2dd-08002b30309d}

Opens kev: HKCU\software\classes\clsid\{35786d3c-b075-49b9-88dd-029876e11c01} Opens key: HKCU\software\classes\clsid\{9113a02d-00a3-46b9-bc5f-

9c04daddd5d7}\shellfolder

HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder Opens key:

Opens key: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}

Opens key:

 $HKLM \setminus software \setminus irrosoft \setminus ir$

49b9-88dd-029876e11c01}

Opens key:

49b9-88dd-029876e11c01}

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9113a02d-

00a3-46b9-bc5f-9c04daddd5d7}\shellfolder

HKLM\software\microsoft\windows\currentversion\explorer\clsid\{9113a02d-Opens key:

00a3-46b9-bc5f-9c04daddd5d7}\shellfolder

HKCU\software\classes\clsid\{b155bdf8-02f0-451e-9a26-Opens key:

ae317cfd7779}\shellfolder

HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\clsid\{b155bdf8-Opens kev:

02f0-451e-9a26-ae317cfd7779}\shellfolder

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{b155bdf8-

02f0-451e-9a26-ae317cfd7779}\shellfolder

HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-Opens key:

8d23b85255bf}\shellfolder

HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder Opens key:

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \clseb{lem:hkcu} \end{tabular} $$ -2.5 \clsid \c$

7ae7-4e32-a8e8-8d23b85255bf}\shellfolder

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{9c73f5e5-

7ae7-4e32-a8e8-8d23b85255bf}\shellfolder

HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-Opens key:

8d23b85255bf}\inprocserver32

HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32 Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89} Opens kev:

HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89} Opens key: Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

001185ad2b89}\treatas

HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

001185ad2b89}\progid

 $HKCR \ clsid \ \{a47979d2-c419-11d9-a5b4-001185ad2b89\} \ \ progid$ Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{a47979d2 - c419 - 11d9 - a5b4 - a5b4$

001185ad2b89}

 $HKCR \setminus \{a47979d2 - c419 - 11d9 - a5b4 - 001185ad2b89\}$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{a47979 \\ d2-c419-11 \\ d9-a5b4-b4797 \\ d2-c419-11 \\ d2-c419-$

001185ad2b89}\progid

Opens key: $HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid$

HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-Opens key:

8d23b85255bf}\treatas

HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\progid

Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\progid

Opens key:

8d23b85255bf}

HKCR\wow6432node\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{9c73f5e5-7ae7-4e32-a8e8-

8d23b85255bf}\progid

HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-Opens key:

001185ad2b89}\inprocserver32

HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

001185ad2b89}\inprochandler32

Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32

Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

001185ad2b89}\inprochandler

HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler Opens kev: Opens key: $HKCR \ wow 6432 node \ clsid \ \{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf\} \ \ progid$

HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-Opens key:

8d23b85255bf}\inprochandler32

Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler32

Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-

8d23b85255bf}\inprochandler

Opens key: $\label{lem:hkcr} $$ HKCR\clsid_{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler $$ $$$ Opens key:

a8e8-8d23b85255bf}

HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27} Opens key:

Opens kev: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27} Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\treatas

HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-Opens key:

2299f0398e27}\progid

Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}

HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\progid

HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid Opens kev:

Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\inprocserver32

HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\inprochandler32

HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32 Opens kev:

Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\inprochandler

HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler Opens key: Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}

HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07} Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-Opens kev:

00aa00341d07}\treatas

Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-

00aa00341d07}\progid

Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid

HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-Opens key:

00aa00341d07}

Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07} HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-Opens key:

00aa00341d07}\progid

HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid Opens key:

HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-Opens key:

00aa00341d07}\inprocserver32

Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32

HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-Opens key:

00aa00341d07}\inprochandler32

HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32 Opens key:

HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-Opens key:

00aa00341d07}\inprochandler

HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler Opens kev:

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{7007acc7-3202-11d1-aad2-11d$ Opens key:

00805fc1270e}\inprocserver32

HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32 Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key:

Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\treatas

 $HKCR \ clsid \ \{7007acc7-3202-11d1-aad2-00805fc1270e\} \ treat as$ Opens key: Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\progid

Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}

Opens key:

HKCR\wow6432node\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key: HKCU\software\classes\wow6432node\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\progid

Opens key: HKCR\wow6432node\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\progid

Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\inprochandler32

Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprochandler32

HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-Opens kev:

00805fc1270e}\inprochandler

HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprochandler Opens kev:

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-

aad2-00805fc1270e}

Opens kev:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ control panel \ namespace \ \{7007acc7-3202-12014, 12014,$

11d1-aad2-00805fc1270e}

Opens kev:

HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-

11d1-aad2-00805fc1270e}

HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d} Opens kev:

Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d} Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-

3aea-1069-a2de-08002b30309d}

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ large \ make us to mization software \ microsoft \ make \ make$

HKLM\svstem\currentcontrolset\control\mui\stringcachesettings Opens key:

Opens key: HKCU\software\classes\local settings\muicache\16\52c64b7e

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-

3202-11d1-aad2-00805fc1270e}

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{20d04fe0-3aea-1069-a2d8-08002b30309d\}$ Opens key:

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d} Opens key:

Opens kev:

 $HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ hidedesk topic on s \ new start panel$

Opens key:

Opens key: HKLM\software\microsoft\windows

nt\currentversion\softwareprotectionplatform

HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b} Opens kev:

Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b} Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-

355b7f55341b}\treatas

Opens key: $HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas$ Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-

355b7f55341b}\progid

Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-

355b7f55341b}

Opens key: HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b} Opens key: HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-

355b7f55341b}\progid

Opens key: HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid

Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-

355b7f55341b}\inprocserver32

HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-

355b7f55341b}\inprochandler32

HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32 Opens key:

HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-Opens kev:

355b7f55341b}\inprochandler

 $HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler$ Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8} Opens key:

HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8} Opens key: Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-

a0b2badd77c8}\treatas

HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-

a0b2badd77c8}\progid

 $HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid$ Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{a2a9545d - a0c2 - 42b4 - 9708 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - a0c2$ a0b2badd77c8}

HKCR\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-

a0b2badd77c8}\progid

 $HKCR\wow6432 node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid$ Opens key:

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{a2a9545d - a0c2 - 42b4 - 9708 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - a$ Opens key:

a0b2badd77c8}\inprocserver32

 $HKCR \c1sid \a2a9545d-a0c2-42b4-9708-a0b2badd77c8 \nprocserver32$ Opens key:

HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-Opens key:

a0b2badd77c8}\inprochandler32

HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler32 Opens key:

Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-

a0b2badd77c8}\inprochandler

 $HKCR \ clsid \ \{a2a9545d-a0c2-42b4-9708-a0b2badd77c8\} \ \ in prochandler$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{90aa3a4e-1cba-4233-b8bb-535773d48449\}$

HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449} Opens kev: Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}\treatas

Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-Opens key:

535773d48449}\progid

HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}

Opens kev:

HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449} Opens kev: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-Opens key:

535773d48449}\progid

Opens key: HKCR\wow6432node\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 kev:

Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}\inprochandler32

HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler32 Opens key:

Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-

```
535773d48449}\inprochandler
                                    HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler
  Opens kev:
  Opens key:
                                    HKCU\software\classes\applications\calc.exe
  Opens key:
                                    HKCR\applications\calc.exe
  Opens key:
                                    HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
                                    HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
  Opens key:
                                    HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
  Opens key:
0000f87a470c}\treatas
                                    HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
  Opens key:
                                    HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
  Opens key:
0000f87a470c}\progid
                                    HKCR\clsid\dd313e04-feff-11d1-8ecd-0000f87a470c\\\progid
  Opens key:
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}
  Opens key:
                                    HKCR\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
                                    HKCU\software\classes\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-
  Opens key:
0000f87a470c}\progid
  Opens key:
                                    HKCR\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid
  Opens key:
                                    HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32
  Opens key:
                                    HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32
  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
  Opens key:
                                    HKCR\clsid\\\{dd313e04-feff-11d1-8ecd-0000f87a470c\\\}\inprochandler
  Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follows folders
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
                                   HKLM\software\microsoft\windows\currentversion\explorer\user shell
  Opens key:
folders
  Opens key:
                                    HKLM\software\microsoft\ctf\knownclasses
                                   \label{lem:hklmsoftware} \verb+ HKLM \software \microsoft \windows nt \current version \cite{lem:hklmsoftware} in the execution \cite{lem:hklmsoftware} and \cite{lem:hklmsoftware} in the execution \cite{lem:hklmsoftware} and \ci
  Oueries value:
options[disableusermodecallbackfilter]
  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]
  Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ [transparentenabled]
                                   HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                                    HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:
  Oueries value:
                                    HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
                                    HKCU\control panel\desktop[preferreduilanguages]
  Oueries value:
  Queries value:
                                   HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                    HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                    HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[1be5bc13fd1cf615a95feec0c5b7fd13]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
                                    HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
```

Oueries value:

Oueries value:

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[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\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000003 \ [storesserviceclassinfo] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries 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\00000000004[providerid]
 Queries 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]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names \pace_catalog 5 \catalog_entries \names \names \pace_catalog 5 \catalog_entries \names \$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog\_entries \ (00000000004[storesserviceclass info]) \ (catalog\_entries) \ 
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000004 [provider info]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000005[providerid]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 \ [address family]
  Queries value:
Oueries 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\00000000005[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[displaystring]
  Queries value:
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000006 \ [address family]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (00000000000006 \ [enabled]) \ (enabled)
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 numhandle buckets]
                                   HKCU\software\microsoft\windows\currentversion\action
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881\}.check.100[checksetting]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[lastknownstate]
                                   HKCU\software\microsoft\windows\currentversion\action
  Queries value:
center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101[checksetting]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}[lastknownstate]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\action
center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100[checksetting]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
                                   HKLM\system\currentcontrolset\services\winsock\setup
  Oueries value:
migration\providers\tcpip[winsock 2.0 provider id]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[image path]
  Queries value:
                                   HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicv[enabled]
  Queries value:
                                   HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
                                   HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Oueries value:
  Oueries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
```

HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]

HKLM\software\microsoft\cryptography[machineguid]

HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

Queries value: Queries value:

Oueries value: HKLM\system\currentcontrolset\computername\activecomputername[computername] Oueries value: HKLM\system\setup[oobeinprogress] Queries value: HKLM\system\setup[systemsetupinprogress] Oueries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Queries value: HKLM\system\currentcontrolset\services\bfe[imagepath] Oueries value: HKLM\system\currentcontrolset\services\bfe[type] Oueries value: HKLM\system\currentcontrolset\services\bfe[start] Oueries value: HKLM\system\currentcontrolset\services\bfe[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\bfe[tag] Oueries value: HKLM\system\currentcontrolset\services\bfe[dependonservice] Queries 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] Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action] Queries value: Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type] Queries 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\winsock2\parameters[current_protocol_catalog] Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 4 \ 0000000000010 \ [packed catalog item]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_entries64\000000000008[packedcatalogitem] Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries 64 \ 000000000007 \ [packed catalog item]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_\catalog_entries64\000000000005[packedcatalogitem] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_\catalog_entries64\0000000000002[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\00000000001[packedcatalogitem] Queries value: Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000000f[providerid] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid] Oueries value: Queries value: 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] Oueries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0] Queries value: Queries value: $HKLM \verb|\software\m| icrosoft \verb|\cryptography\defaults\provider\m| base$ cryptographic provider v1.0[type] Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base cryptographic provider v1.0[image path] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2]

HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]

Queries value:

Queries value: Oueries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

```
Oueries value:
                          HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]
                          HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
 Queries value:
                          HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
 Oueries value:
                          HKLM\system\currentcontrolset\services\browser[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\browser[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\browser[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\browser[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\browser[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\browser[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\browser[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\browser[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\browser[objectname]
                          HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\rpcss[objectname]
 Queries value:
                          HKLM\svstem\currentcontrolset\services\wuauserv[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\wuauserv[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wuauserv[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wuauserv[requiredprivileges]
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[type]
                          HKLM\system\currentcontrolset\services\cryptsvc[start]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[group]
                          HKLM\system\currentcontrolset\services\cryptsvc[objectname]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
 Queries value:
                          HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
                          HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
 Queries value:
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
 Queries value:
folders[cache]
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Oueries value:
options[disablelocaloverride]
                          HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\compatibility32[cmd]
                          HKLM\system\currentcontrolset\control\cmf\config[system]
 Queries value:
                          HKLM\system\currentcontrolset\services\gpsvc[imagepath]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\gpsvc[type]
                          HKLM\system\currentcontrolset\services\gpsvc[start]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\gpsvc[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\gpsvc[tag]
 Queries value:
                          HKLM\system\currentcontrolset\services\gpsvc[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\gpsvc[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\gpsvc[group]
                          HKLM\system\currentcontrolset\services\gpsvc[objectname]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]
                          HKLM\system\currentcontrolset\services\dnscache[imagepath]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache[type]
                          HKLM\system\currentcontrolset\services\dnscache[start]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache[tag]
                          {\it HKLM \ } system \ \verb| current control set \ \verb| services \ \verb| dns cache[dependon service]|
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache[group]
                          HKLM\system\currentcontrolset\services\dnscache[objectname]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]
 Oueries value:
                          HKLM \setminus system \setminus current control set \setminus services \setminus efs \setminus trigger info \setminus 0 [type]
 Queries value:
                          HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
 Oueries value:
                          HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
 Oueries value:
 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\svstem\currentcontrolset\services\hidserv\triggerinfo\0ſdatatype11
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
 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]
```

HKLM\system\currentcontrolset\services\ikeext[imagepath]

Queries value:

```
Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[start]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
 Queries value:
                         HKLM\system\currentcontrolset\services\ikeext[tag]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[dependonservice]
 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:
 Oueries value:
                         HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\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]
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
 Oueries 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]
 Oueries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
 Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
                         HKLM\system\currentcontrolset\services\policyagent[imagepath]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent[type]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent[start]
 Oueries value:
                         {\tt HKLM \ } system \verb| current control set \verb| services \verb| policyagent[error control]|
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent[tag]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent[dependonservice]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[dependongroup]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent[group]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent[objectname]
                         HKLM \setminus system \setminus current control set \setminus services \setminus sens rsvc \setminus trigger info \setminus 0 \ [action]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
 Queries value:
                         HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
 Oueries value:
                         HKLM \setminus system \setminus current control set \setminus services \setminus sens rsvc \setminus trigger info \setminus 0 \ [data type 0]
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
 Queries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype3]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
 Queries value:
Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
```

 $HKLM \setminus system \setminus current control set \setminus services \setminus trigger info \setminus 0 [data type 0]$

Oueries value:

Queries value:

Oueries value:

Oueries value:

Oueries value:

Queries value:

 $\label{lem:lem:queries} Queries \ value: \\ HKLM \ system \ (current control set \ services \ wers v c \ trigger in fo \ 0 \ [action] \\$

HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]

HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]

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

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

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

```
Oueries 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]
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
  Queries value:
  Oueries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
  Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
  Oueries value:
  Oueries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
  Oueries value:
  Queries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
  Oueries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
  Oueries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
  Oueries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
  Queries value:
                                  HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion[devicepath]
                                  HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:
  Queries value:
                                  HKLM\system\currentcontrolset\control\idconfigdb[currentconfig]
  Oueries value:
HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo[dockingstate]
                                  HKLM\system\currentcontrolset\control\idconfigdb\hardware
  Oueries value:
profiles\0001[hwprofileguid]
                                  HKLM\system\currentcontrolset\control\idconfigdb\hardware
  Queries value:
profiles\0001[friendlyname]
  Oueries value:
                                  HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[]
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders[suppressionpolicv]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders[]
  Queries value:
b075-49b9-88dd-029876e11c01}[suppressionpolicy]
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Oueries value:
beb064c98683}\shellfolder[attributes]
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Oueries value:
beb064c98683}\shellfolder[callforattributes]
  Queries value:
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[restrictedattributes]
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Oueries value:
beb064c98683}\shellfolder[wantsfordisplay]
  Oueries value:
00a3-46b9-bc5f-9c04daddd5d7}[suppressionpolicy]
HKLM \ software \ microsoft \ windows \ current version \ explorer \ more \ more \ delegate folders \ \{b155bdf8-the microsoft \ more 
02f0-451e-9a26-ae317cfd7779}[suppressionpolicy]
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Queries value:
beb064c98683}\shellfolder[hidefolderverbs]
  Queries value:
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[usedrophandler]
  Queries value:
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[wantsforparsing]
  Queries value:
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[wantsparsedisplayname]
  Queries value:
                                  HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[queryforoverlay]
                                  HKLM\software\microsoft\windows
  Oueries value:
d6ec3f16059f[referralid]
                                  HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[attributes]
                                  HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[callforattributes]
                                  HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[restrictedattributes]
                                  HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[wantsfordisplay]
```

```
HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Queries value:
029876e11c01}\shellfolder[hidefolderverbs]
                                      HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[]
  Oueries value:
  Queries value:
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[mapnetdriveverbs]
  Queries value:
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[queryforinfotip]
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Oueries value:
beb064c98683}\shellfolder[hideinwebview]
  Oueries value:
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[hideondesktopperuser]
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Queries value:
beb064c98683}\shellfolder[wantsaliasednotifications]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[usedrophandler]
  Queries value:
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[wantsforparsing]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Queries value:
029876e11c01}\shellfolder[wantsparsedisplayname]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Queries value:
029876e11c01}\shellfolder[queryforoverlay]
  Queries value:
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[mapnetdriveverbs]
                                      HKCR\clsid\{33c4643c-7811-46fa-a89a-
  Queries value:
768597bd7223}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]
  Queries value:
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Queries value:
beb064c98683}\shellfolder[wantsuniversaldelegate]
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Oueries value:
beb064c98683}\shellfolder[nofilefolderjunction]
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Oueries value:
beb064c98683}\shellfolder[pintonamespacetree]
                                      HKCR\clsid\{26ee0668-a00a-44d7-9371-
  Queries value:
beb064c98683}\shellfolder[hasnavigationenum]
  Oueries value:
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[queryforinfotip]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[hideinwebview]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Queries value:
029876e11c01}\shellfolder[hideondesktopperuser]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[wantsaliasednotifications]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[wantsuniversaldelegate]
                                      HKCR\clsid\{33c4643c-7811-46fa-a89a-
  Oueries value:
768597bd7223}\inprocserver32[threadingmodel]
  Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{26ee0668-a00a-44d7-9371-a00a-44d7-9371-a00a-44d7-9371-a00a-44d7-9371-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a
beb064c98683}1
  Queries value:
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[nofilefolderjunction]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Oueries value:
029876e11c01}\shellfolder[pintonamespacetree]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-
  Queries value:
029876e11c01}\shellfolder[hasnavigationenum]
  Queries value:
                                      HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[sortorderindex]
                                      HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
  Oueries value:
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{35786d3c-b075-49b9-88dd-
029876e11c01}]
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Queries value:
9c04daddd5d7}\shellfolder[attributes]
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Queries value:
9c04daddd5d7}\shellfolder[callforattributes]
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Oueries value:
9c04daddd5d7}\shellfolder[restrictedattributes]
                                      HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}[sortorderindex]
  Queries value:
  Oueries value:
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[wantsfordisplay]
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Oueries value:
9c04daddd5d7}\shellfolder[hidefolderverbs]
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Oueries value:
9c04daddd5d7}\shellfolder[usedrophandler]
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Queries value:
9c04daddd5d7}\shellfolder[wantsforparsing]
  Oueries value:
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[wantsparsedisplayname]
  Oueries value:
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[queryforoverlay]
  Oueries value:
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[mapnetdriveverbs]
                                      HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Oueries value:
9c04daddd5d7}\shellfolder[queryforinfotip]
```

```
HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Queries value:
9c04daddd5d7}\shellfolder[hideinwebview]
  Oueries value:
                                       HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[hideondesktopperuser]
                                       HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Oueries value:
9c04daddd5d7}\shellfolder[wantsaliasednotifications]
  Queries value:
                                       HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                       HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[nofilefolderjunction]
                                       HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
  Oueries value:
9c04daddd5d7}\shellfolder[pintonamespacetree]
  Queries value:
                                       HKCR\clsid\{9113a02d-00a3-46b9-bc5f-
9c04daddd5d7}\shellfolder[hasnavigationenum]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9113a02d-00a3-46b9-bc5f-
9c04daddd5d711
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[attributes]
                                      HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[callforattributes]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[restrictedattributes]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
ae317cfd7779}\shellfolder[wantsfordisplay]
                                      HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[hidefolderverbs]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[usedrophandler]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[wantsforparsing]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[wantsparsedisplayname]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[queryforoverlay]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[mapnetdriveverbs]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Oueries value:
ae317cfd7779}\shellfolder[queryforinfotip]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[hideinwebview]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[hideondesktopperuser]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-}
  Queries value:
ae317cfd7779}\shellfolder[wantsaliasednotifications]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Queries value:
ae317cfd7779}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
ae317cfd7779}\shellfolder[nofilefolderjunction]
  Queries value:
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
ae317cfd7779}\shellfolder[pintonamespacetree]
                                       HKCR\clsid\{b155bdf8-02f0-451e-9a26-
  Oueries value:
ae317cfd7779}\shellfolder[hasnavigationenum]
  Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{b155bdf8-02f0-451e-9a26-164e, 164e-164e, 164e-164
ae317cfd7779}1
  Oueries value:
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[attributes]
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Oueries value:
8d23b85255bf}\shellfolder[callforattributes]
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Queries value:
8d23b85255bf}\shellfolder[restrictedattributes]
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Queries value:
8d23b85255bf}\shellfolder[wantsfordisplay]
  Queries value:
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[hidefolderverbs]
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Queries value:
8d23b85255bf}\shellfolder[usedrophandler]
  Queries value:
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[wantsforparsing]
  Queries value:
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[wantsparsedisplayname]
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Oueries value:
8d23b85255bf}\shellfolder[queryforoverlay]
  Queries value:
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[mapnetdriveverbs]
  Queries value:
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[queryforinfotip]
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Oueries value:
8d23b85255bf}\shellfolder[hideinwebview]
                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Queries value:
8d23b85255bf}\shellfolder[hideondesktopperuser]
```

HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-

Queries value:

```
8d23b85255bf}\shellfolder[wantsaliasednotifications]
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Oueries value:
8d23b85255bf}\shellfolder[wantsuniversaldelegate]
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Queries value:
8d23b85255bf}\shellfolder[nofilefolderjunction]
  Queries value:
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[pintonamespacetree]
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Oueries value:
8d23b85255bf}\shellfolder[hasnavigationenum]
  Oueries value:
8d23b85255bf}]
  Oueries value:
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\tinprocserver32[]
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Oueries value:
8d23b85255bf}\inprocserver32[loadwithoutcom]
                                    HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
  Queries value:
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  Oueries value:
8d23b85255bf}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
  Queries value:
                                    HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-}
  Oueries value:
2299f0398e27}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
  Oueries value:
2299f0398e27}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
  Queries value:
  Oueries value:
                                    HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{b196b286-bab4-101a-b69c-
  Queries value:
00aa00341d07}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\inprocserver32[loadwithoutcom]
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[]
  Oueries value:
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-
  Oueries value:
00805fc1270e}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-
  Queries value:
00805fc1270e}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e\}[sortorderindex]
                                    HKCR\clsid\{2227a280-3aea-1069-a2de-
  Oueries value:
08002b30309d}[system.itemnamedisplay]
                                    HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[{b725f130-47ef-101a-
  Oueries value:
a5f1-02608c9eebac} 10]
  Queries value:
                                    HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
  Queries value:
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
  Queries value:
                                    HKCU\software\classes\local
settings\muicache\16\52c64b7e[@c:\windows\system32\prnfldr.dll,-8036]
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-
  Oueries value:
00805fc1270e}[system.itemnamedisplay]
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[{b725f130-47ef-101a-
  Queries value:
a5f1-02608c9eebac} 101
  Queries value:
                                    HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
  Oueries value:
                                    HKCU\software\classes\local
settings\muicache\16\52c64b7e[@c:\windows\system32\netshell.dll.-12001
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[system.hideondesktop]
  Oueries value:
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{28636aa6-953d-11d2-
  Queries value:
b5d6-00c04fd918d0} 34]
  Oueries value:
HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} White \
3aea-1069-a2d8-08002b30309d}]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[inactivitvshutdowndelav]
                                    HKLM\software\microsoft\windows
  Queries value:
\verb|nt\current version \verb| software protection platform[| keep running threshold mins]| \\
  Queries value:
                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
  Oueries value:
                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-
  Oueries value:
355b7f55341b}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
  Oueries value:
                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
  Oueries value:
  Oueries value:
                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
  Queries value:
  Oueries value:
                                    HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[inprocserver32]
```

```
\label{local-basis} HKCR \clsid \ \{90 aa 3a 4e - 1cba - 4233 - b8bb - 535773d 48449\} \ \ in procserver 32[]
 Oueries value:
                     HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
 Oueries value:
535773d48449}\inprocserver32[threadingmodel]
                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[]
 Queries value:
                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-
 Oueries value:
0000f87a470c}\inprocserver32[inprocserver32]
                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\nprocserver32[]
 Oueries value:
                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-
 Oueries value:
0000f87a470c}\inprocserver32[threadingmodel]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[programs]
 Queries value:
                     HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common programs]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{9e3995ab-1f9c-4f13-b827-48b24b6c7174}]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}]
                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[appdata]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
                     HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
 Sets/Creates value:
409d6c4515e9}\inprocserver32[threadingmodel]
 Sets/Creates value:
                     HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[]
 Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
                     HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
 Value changes:
 Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000010 \ [packed catalog item]
 Value changes:
Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000006 \ [packed catalog item]
 Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000005 \ [packed catalog item]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Value changes:
Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Value changes:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries 64 \ 000 \ 000 \ 000 \ 000 \ 10 \ [packed catalog item]
 Value changes:
Value changes:
Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries 64 \ 000 000 000 000 7 \ [packed catalog item]
 Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\00000000005[packedcatalogitem]
 Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries 64 \ 000 000 000 000 4 \ [packed catalog item]
 Value changes:
Value changes:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 4 \ 000000000000002 \ [packed catalog item]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_\catalog_entries64\00000000001[packedcatalogitem]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
 Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000005[librarypath]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[librarypath]
 Value changes:
                     HKLM\system\currentcontrolset\services\browser[start]
 Value changes:
                     HKLM\system\currentcontrolset\services\policyagent[start]
```

HKCU\software\classes\local settings\muicache\16\52c64b7e[languagelist]

Value changes:

Value changes:

 $\label{thm:bound} HKCU \software \microsoft \windows \current version \explorer \user as sist \{cebff5cd-ace2-4f4f-9178-9926f41749ea\} \count[hrzr_pgyfrffvba]$