

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 42, Task ID: 166

Task ID:	166
Risk Level:	4
Date Processed:	2016-04-28 12:51:31 (UTC)
Processing Time:	2.34 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\fec00c2e3361c5caf7382f9ea1a7442f.exe"
Sample ID:	42
Type:	basic
Owner:	admin
Label:	fec00c2e3361c5caf7382f9ea1a7442f
Date Added:	2016-04-28 12:44:54 (UTC)
File Type:	PE32:win32:gui
File Size:	193824 bytes
MD5:	fec00c2e3361c5caf7382f9ea1a7442f
SHA256:	153a3296a523ae0f606dfb4cb4178affe97e2f7c4f1faab223ca653e5b74261c
Description:	None

Pattern Matching Results

- 2 PE: Nonstandard section
- 4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\fec00c2e3361c5caf7382f9ea1a7442f.exe
["c:\windows\temp\fec00c2e3361c5caf7382f9ea1a7442f.exe"]	
Creates process:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsq2.tmp\ns3.tmp
["C:\DOCUME~1\Admin\LOCALS~1\Temp\nsq2.tmp\ns3.tmp" "C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe" install]	
Terminates process:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsq2.tmp\ns3.tmp
Terminates process:	C:\WINDOWS\Temp\fec00c2e3361c5caf7382f9ea1a7442f.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp
Creates: C:\DOCUME~1
Creates: C:\DOCUME~1\Admin
Creates: C:\DOCUME~1\Admin\LOCALS~1
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\System.dll
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsq2.tmp\System.dll
Creates: C:\Program Files
Creates: C:\Program Files\Mozilla Maintenance Service
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\nsExec.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\ns3.tmp
Creates: C:\Program Files\Mozilla Maintenance Service\Uninstall.exe
Opens: C:\WINDOWS\Prefetch\FEC00C2E3361C5CAF7382F9EA1A74-21F8108A.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\shfolder.dll
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\
Opens: C:\Documents and Settings
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp
Opens: C:\WINDOWS\Temp\0b2d5dd4-a835-45f9-b4e1-0e10a10eaf5d
Opens: C:\WINDOWS\Temp\fec00c2e3361c5caf7382f9ea1a7442f.exe
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\System.dll
Opens: C:\Program Files\Mozilla Maintenance Service
Opens: C:\WINDOWS\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\nsExec.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\ns3.tmp
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\sysrest.sdb
Opens: C:\Documents and Settings\Admin\Local Settings
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsq2.tmp\ns3.tmp.Manifest
Opens: C:\WINDOWS\Prefetch\NS3.TMP-0829E87F.pf
Opens: C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe
Opens: C:\Program Files\Mozilla Maintenance Service\Uninstall.exe
Opens: C:\Program Files\Mozilla Maintenance Service\Uninstall.exe
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\System.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\nsExec.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\ns3.tmp
Writes to: C:\Program Files\Mozilla Maintenance Service\Uninstall.exe
Reads from: C:\WINDOWS\Temp\fec00c2e3361c5caf7382f9ea1a7442f.exe
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\ns3.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\nsExec.dll
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsq2.tmp\System.dll

Windows Registry Events

Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-

```

806d6172696f}\
  Creates key:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice
  Creates key:      HKLM\software\mozilla\maintenanceservice
  Deletes value:    HKLM\software\mozilla\maintenanceservice[ffprefetchdisabled]
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\fec00c2e3361c5caf7382f9ea1a7442f.exe
  Opens key:        HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:        HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:        HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:        HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:        HKLM\system\currentcontrolset\control\session manager
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:        HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:        HKLM\system\currentcontrolset\control\error message instrument
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:        HKLM\
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:        HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:        HKLM\system\setup
  Opens key:        HKCU\
  Opens key:        HKCU\software\policies\microsoft\control panel\desktop
  Opens key:        HKCU\control panel\desktop
  Opens key:        HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:        HKLM\software\microsoft\ole
  Opens key:        HKCR\interface
  Opens key:        HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:

```

HKLM\software\microsoft\ctf\compatibility\fec00c2e3361c5caf7382f9ea1a7442f.exe
 Opens key: HKLM\software\microsoft\ctf\systemshared\
 Opens key: HKCU\keyboard layout\toggle
 Opens key: HKLM\software\microsoft\ctf\
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\shfolder.dll
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
 Opens key:
 HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-a2d8-08002b30309d}
 Opens key: HKCU\software\classes\
 Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
 Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\setupapi.dll
 Opens key: HKLM\system\currentcontrolset\control\minint
 Opens key: HKLM\system\wpa\pnp
 Opens key: HKLM\software\microsoft\windows\currentversion\setup
 Opens key: HKLM\software\microsoft\windows\currentversion
 Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
 Opens key: HKLM\software\policies\microsoft\system\dnsclient
 Opens key: HKLM\software\microsoft\rpc\pagedbuffers
 Opens key: HKLM\software\microsoft\rpc
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\fec00c2e3361c5caf7382f9ea1a7442f.exe\rpcthreadpoolthrottle
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
 Opens key: HKCU\software\classes\drive\shellex\folderextensions
 Opens key: HKCR\drive\shellex\folderextensions
 Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
 Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
 Opens key:
 HKCU\software\classes\directory
 Opens key: HKCR\directory
 Opens key: HKCU\software\classes\directory\curver
 Opens key: HKCR\directory\curver
 Opens key: HKCR\directory\
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\system
 Opens key: HKCU\software\classes\directory\shellex\iconhandler
 Opens key: HKCR\directory\shellex\iconhandler
 Opens key: HKCU\software\classes\directory\clsid
 Opens key: HKCR\directory\clsid
 Opens key: HKCU\software\classes\folder
 Opens key: HKCR\folder
 Opens key: HKCU\software\classes\folder\clsid
 Opens key: HKCR\folder\clsid
 Opens key: HKLM\software\mozilla\maintenanceservice
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\system.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\nsexec.dll

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\ms3.tmp
Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\ms3.tmp
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[fec00c2e3361c5caf7382f9ea1a7442f]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
 compatibility[fec00c2e3361c5caf7382f9ea1a7442f]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value: HKLM\system\setup[systemsetupinprogress]
 Queries value: HKCU\control panel\desktop[multiuilanguageid]
 Queries value: HKCU\control panel\desktop[smoothscroll]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[criticalsectiontimeout]
 Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Queries value: HKCR\interface[interfacehelperdisableall]
 Queries value: HKCR\interface[interfacehelperdisableallforole32]
 Queries value: HKCR\interface[interfacehelperdisabletypelib]
 Queries value: HKCR\interface\{00020400-0000-0000-c000-
 000000000046}[interfacehelperdisableall]
 Queries value: HKCR\interface\{00020400-0000-0000-c000-
 000000000046}[interfacehelperdisableallforole32]
 Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
 Queries value: HKCU\keyboard layout\toggle[language hotkey]
 Queries value: HKCU\keyboard layout\toggle[hotkey]
 Queries value: HKCU\keyboard layout\toggle[layout hotkey]
 Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
 Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
Queries value: HKLM\system\wpa\pnp[seed]
Queries value: HKLM\system\setup[osloaderpath]
Queries value: HKLM\system\setup[systempartition]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
Queries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]
Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[data]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[generation]
Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]

Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
Queries value: HKCR\directory[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemsizes]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemsizes]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsizes]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]
Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsizes]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemsizes]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfileaname]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[ns3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[ns3]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayname]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[uninstallstring]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayicon]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayversion]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[publisher]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[comments]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[nomodify]
Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[estimatedsize]
Sets/Creates value: HKLM\software\mozilla\maintenanceservice[attempted]
Sets/Creates value: HKLM\software\mozilla\maintenanceservice[installed]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]