

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 154, Task ID: 615

Task ID:	615
Risk Level:	6
Date Processed:	2016-04-28 13:03:58 (UTC)
Processing Time:	61.37 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e8ba5491fe0eaed78c366b525066ffcd.exe"
Sample ID:	154
Type:	basic
Owner:	admin
Label:	e8ba5491fe0eaed78c366b525066ffcd
Date Added:	2016-04-28 12:45:06 (UTC)
File Type:	PE32:win32:gui
File Size:	57961 bytes
MD5:	e8ba5491fe0eaed78c366b525066ffcd
SHA256:	4c57fe49ae3bd0bd9829bd43e8d50a7e411a4c4b75f5c2a036d6c084b6bdb381
Description:	None

Pattern Matching Results

- 2 PE: Nonstandard section
- 5 Creates process in suspicious location
- 6 Renames file on boot
- 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\e8ba5491fe0eaed78c366b525066ffcd.exe
["c:\windows\temp\e8ba5491fe0eaed78c366b525066ffcd.exe"]	
Creates process:	C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Au_.exe
["C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Au_.exe" _?=c:\windows\temp\]	
Terminates process:	C:\WINDOWS\Temp\e8ba5491fe0eaed78c366b525066ffcd.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 mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.AHH
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.MMF
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.MMF.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.MMF.IC
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\new1.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\~nsu.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\~nsu.tmp\Au_.exe
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\new2.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\new3.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\nsz3.tmp\UserInfo.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsz3.tmp\LangDLL.dll
Opens: C:\WINDOWS\Prefetch\E8BA5491FE0EAED78C366B525066F-01B29FF6.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\nsw1.tmp
Opens: C:\WINDOWS\Temp\4d53dd74-5e66-4097-a132-ccab79b6d216
Opens: C:\WINDOWS\Temp\e8ba5491fe0aed78c366b525066ffcd.exe
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\~nsu.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Au_.exe
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\~nsu.tmp\Au_.exe
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:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Au_.exe.Manifest
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Au_.exe.Config
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Bu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Cu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Du_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Eu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Fu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Gu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Hu_.exe
Opens: C:\WINDOWS\Prefetch\AU_.EXE-34E9686B.pf
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Iu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Ju_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Ku_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Lu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Mu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Nu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Ou_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Pu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Qu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Ru_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Su_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Tu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Uu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Vu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Wu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp Xu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Yu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp\Zu_.exe
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\~nsu.tmp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsf2.tmp
Opens: C:\WINDOWS
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsz3.tmp
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\nsz3.tmp\UserInfo.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsz3.tmp\LangDLL.dll
Opens: C:\WINDOWS\system32\MSCTIME.IME
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\system32\MSIMTF.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\~nsu.tmp\Au_.exe
Writes to: C:\Documents and Settings\Admin\Local
Settings\Temp\nsz3.tmp\UserInfo.dll

Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsz3.tmp\LangDLL.dll
Reads from: C:\WINDOWS\Temp\e8ba5491fe0eae78c366b525066ffcd.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\~nsu.tmp\Au_.exe
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsw1.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsf2.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsz3.tmp

Windows Registry Events

Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Creates key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\e8ba5491fe0eae78c366b525066ffcd.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\e8ba5491fe0eae78c366b525066ffcd.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\applications\e8ba5491fe0aed78c366b525066ffcd.exe
 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\e8ba5491fe0aed78c366b525066ffcd.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\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\au_.exe
 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-
7c29ddec3f}
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\au_.exe
Opens key: HKLM\software\microsoft\ctf\compatibility\au_.exe
Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\au_.exe
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\au_.exe\rpcthreadpoolthrottle
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\userinfo.dll
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\zinsmath
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\langdll.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime
 Opens key: HKCU\software\microsoft\ctf
 Opens key: HKLM\software\microsoft\ctf\systemshared
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uxtheme.dll
 Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
 Opens key: HKCU\software\microsoft\ctf\langbaraddin\
 Opens key: HKLM\software\microsoft\ctf\langbaraddin\
 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[e8ba5491fe0aed78c366b525066ffcd]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[e8ba5491fe0aed78c366b525066ffcd]
 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\system\currentcontrolset\control\session
manager[pendingfilerenameoperations2]
Queries value: HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
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}[itemsizedata]
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}[itemsizedata]
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-7c29ddec3f}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddec3f}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddec3f}[itemsizedata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddec3f}[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}[itemsizedata]
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}[itemsizedata]
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[logfile]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[au_
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[au_
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]

Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Sets/Creates value: HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}[baseclass]
Value changes: HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]