Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 132, Task ID: 527

Task ID:	527
Risk Level:	1
Date Processed:	2016-04-28 13:01:23 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.exe"
Sample ID:	132
Type:	basic
Owner:	admin
Label:	2a2824f06d8aa50626c0ce6d634603be
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	414810 bytes
MD5:	2a2824f06d8aa50626c0ce6d634603be
SHA256:	499fb3cf2e5aa193e470b23a01ccde14d3414904419844fb2c7954ed0b1f45a6
Description:	None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\2a2824f06d8aa50626c0ce6d634603be.exe ["c:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.exe"]

Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\is-H44E3.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp ["C:\DOCUME~1\Admin\LOCALS~1\Temp\is-H44E3.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp" /SL5="$100CE,168902,61952,c:\windows\temp\2a2824f06d8aa50626c0ce6d634603be.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-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EGH

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\is-H44E3.tmp

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\is-H44E3.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp_isetup

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp_isetup_RegDLL.tmp

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp_isetup_shfoldr.dll

Opens: C:\WINDOWS\Prefetch\2A2824F06D8AA50626C0CE6D63460-26D4E27A.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\Temp\2a2824f06d8aa50626c0ce6d634603be.exe
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
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\system32\netmsg.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\is-H44E3.tmp
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\is-H44E3.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb
Opens: C:\
Opens: C:\Documents and Settings
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\is-H44E3.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp.Manifest
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\is-H44E3.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp.Config
Opens: C:\WINDOWS\Prefetch\2A2824F06D8AA50626C0CE6D63460-2FBD3BBC.pf
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp_isetup
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp_isetup_shfoldr.dll
Opens: C:\WINDOWS\system32\shfolder.dll
Opens: C:\WINDOWS\Fonts\sserife.fon
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\Documents and Settings\Admin\Start Menu\desktop.ini
Opens: C:\Documents and Settings\Admin\Start Menu
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
Opens: C:\WINDOWS\Fonts\verdanab.ttf
Opens: C:\WINDOWS\system32\clbcatq.dll
Opens: C:\WINDOWS\system32\comres.dll
Opens: C:\WINDOWS\Registration\R000000000007.clb
Opens: C:\WINDOWS\system32\browseui.dll
Opens: C:\WINDOWS\system32\browseui.dll.123.Manifest
Opens: C:\WINDOWS\system32\browseui.dll.123.Config
Opens: C:\WINDOWS\system32\riched20.dll
Opens: C:\WINDOWS\win.ini
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\is-H44E3.tmp\2a2824f06d8aa50626c0ce6d634603be.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp_isetup_RegDLL.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\is-OIIG9.tmp_isetup_shfoldr.dll
Reads from: C:\WINDOWS\Temp\2a2824f06d8aa50626c0ce6d634603be.exe
Reads from: C:\WINDOWS\system32\shell32.dll
Reads from: C:\Documents and Settings\Admin\Start Menu\desktop.ini
Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
Reads from: C:\WINDOWS\Registration\R000000000007.clb
Reads from: C:\WINDOWS\win.ini

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\2a2824f06d8aa50626c0ce6d634603be.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\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.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\comctl32.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\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
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\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\system\setup
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\2a2824f06d8aa50626c0ce6d634603be.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\imm
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
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: 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: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\2a2824f06d8aa50626c0ce6d634603be.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\2a2824f06d8aa50626c0ce6d634603be.tmp
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mpr.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key:
HKLM\software\microsoft\ctf\compatibility\2a2824f06d8aa50626c0ce6d634603be.tmp
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows nt\currentversion
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\2a2824f06d8aa50626c0ce6d634603be.tmp
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: 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: 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\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\2a2824f06d8aa50626c0ce6d634603be.tmp\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\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: HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comres.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll
Opens key: HKLM\software\microsoft\com3\debug
Opens key: HKLM\software\classes
Opens key: HKU\
Opens key: HKCR\clsid
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver32
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver32
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\browseui.dll
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserverx86
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver32
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver32
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandler32
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandler32
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandlerx86
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler32
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\riched20.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\windows
Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\{f5a6a617-1a5c-46bd-b44d-5660e337507f}_is1
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{f5a6a617-1a5c-46bd-b44d-5660e337507f}_is1
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[2a2824f06d8aa50626c0ce6d634603be]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[2a2824f06d8aa50626c0ce6d634603be]
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\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: 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\setup[systemsetupinprogress]
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: 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]
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}[itemsize]
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}[itemsize]
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}[itemsize]
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}[itemsize]
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}[itemsize]
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[logfilename]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\microsoft\windows nt\currentversion[registeredowner]
Queries value: HKLM\software\microsoft\windows nt\currentversion[registeredorganization]
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: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[start menu]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common start menu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[recent]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[fonts]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[programs]
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:
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:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[appid]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[appid]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[appid]
Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[alwaysdropup]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewwatermark]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial
tur,162]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[helv]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[helvetica]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms shell dlg 2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tms rmn]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms shell dlg]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[programs]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]