# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 221, Task ID: 885

| | |
|---|---|
| Task ID: | 885 |
| Risk Level: | 3 |
| Date Processed: | 2016-04-28 13:11:44 (UTC) |
| Processing Time: | 3.06 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\1aca077963eb842ac865c50dd866d52c.exe" |
| | |
| Sample ID: | 221 |
| Type: | basic |
| Owner: | admin |
| Label: | 1aca077963eb842ac865c50dd866d52c |
| Date Added: | 2016-04-28 12:45:13 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 989832 bytes |
| MD5: | 1aca077963eb842ac865c50dd866d52c |
| SHA256: | aa67952a7266af5c575c7acf194ff30866fe5cf8ea7f09049dc94c1ee15b0850 |
| Description: | None |

## Pattern Matching Results

3 Long sleep detected
1 YARA score 1

## Static Events

| | |
|---|---|
| YARA rule hit: | OLE2 |
| YARA rule hit: | Nonexecutable |

## Process/Thread Events

Creates process: C:\windows\temp\1aca077963eb842ac865c50dd866d52c.exe
["C:\windows\temp\1aca077963eb842ac865c50dd866d52c.exe" ]
Terminates process: C:\Windows\Temp\1aca077963eb842ac865c50dd866d52c.exe

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \KernelObjects\MaximumCommitCondition
Creates event: \Sessions\1\BaseNamedObjects\OleDfRoot87E34D5F57643F6B
Creates semaphore: \Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?
1ACA077963EB842AC865C50DD866D52C.EXE

## File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\~DF2A88ACAD004F7CA3.TMP
Opens: C:\Windows\Prefetch\1ACA077963EB842AC865C50DD866D-B7842CC0.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\windows\temp\MSVBVM60.DLL
Opens: C:\Windows\SysWOW64\msvbvm60.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll

Opens: C:\Windows\Temp\1aca077963eb842ac865c50dd866d52c.exe
Opens: C:\windows\temp\1aca077963eb842ac865c50dd866d52c.exe.cfg
Opens: C:\windows\temp\SXS.DLL
Opens: C:\Windows\SysWOW64\sxs.dll
Opens: C:\Windows\System32\C_932.NLS
Opens: C:\Windows\System32\C_949.NLS
Opens: C:\Windows\System32\C_950.NLS
Opens: C:\Windows\System32\C_936.NLS
Opens: C:\windows\temp\CRYPTSP.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\windows\temp\RpcRtRemote.dll
Opens: C:\Windows\SysWOW64\RpcRtRemote.dll
Opens: C:\windows\temp\1aca077963eb842ac865c50dd866d52c.exe.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens: C:\Windows\SysWOW64\aloahapopup.dialogs
Opens: C:\Windows\Fonts\sserife.fon
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens: C:\windows\temp\aloahasaver.ocx
Opens: C:\Windows\SysWOW64\aloahasaver.ocx
Opens: C:\Windows\system\aloahasaver.ocx
Opens: C:\Windows\aloahasaver.ocx
Opens: C:\Windows\SysWOW64\Wbem\aloahasaver.ocx
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\aloahasaver.ocx
Opens: C:\Windows\WINHELP.INI
Opens: C:\Windows\SysWOW64\.HLP
Opens: C:\Windows\Help\.HLP
Opens: C:\Users\Admin\AppData\Local\Temp\~DF2A88ACAD004F7CA3.TMP
Reads from: C:\Windows\Temp\1aca077963eb842ac865c50dd866d52c.exe
Deletes: C:\Users\Admin\AppData\Local\Temp\~DF2A88ACAD004F7CA3.TMP

# Windows Registry Events

Creates key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}
Creates key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5
Creates key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags
Creates key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0
Creates key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32
Creates key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir
Creates key: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
Creates key: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
Creates key: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
Creates key: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
Creates key: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\progid
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\localserver32
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\typelib
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\version
Creates key: HKCR\pdfsaver.remotecontrol
Creates key: HKCR\pdfsaver.remotecontrol\clsid
Creates key: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}
Creates key: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-

b42282ece401}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\forward
Creates key: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}
Creates key: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\forward
Creates key: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}
Creates key: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\forward
Creates key: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}
Creates key: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\forward
Creates key: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}
Creates key: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\forward
Creates key: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\implemented categories
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\programmable
Creates key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\implemented categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
Deletes value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\localserver32[threadingmodel]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9
Opens key: HKCR\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9
Opens key: HKCU\software\classes\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9\win32
Opens key: HKCR\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9\win32
Opens key: HKCU\software\classes\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9
Opens key: HKCR\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9
Opens key: HKCU\software\classes\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9\win32
Opens key: HKCR\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9\win32
Opens key: HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0
Opens key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0
Opens key: HKCU\software\classes\typelib
Opens key: HKCR\typelib
Opens key: HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}
Opens key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}
Opens key: HKLM\software\classes
Opens key: HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5
Opens key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5
Opens key: HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags
Opens key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags
Opens key: HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32
Opens key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32
Opens key: HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir
Opens key: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir
Opens key: HKCU\software\classes\wow6432node\interface
Opens key: HKCR\wow6432node\interface
Opens key: HKCU\software\classes\wow6432node\interface\{e194c84a-c2c5-4be2-a499-

7b32bb445d93}
Opens key: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
Opens key: HKCU\software\classes\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
Opens key: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
Opens key: HKCU\software\classes\interface
Opens key: HKCR\interface
Opens key: HKCU\software\classes\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
Opens key: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
Opens key: HKCU\software\classes\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
Opens key: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
Opens key: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\localserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\typelib
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\version
Opens key: HKCU\software\classes\pdfsaver.remotecontrol
Opens key: HKCR\pdfsaver.remotecontrol
Opens key: HKCU\software\classes\pdfsaver.remotecontrol\clsid
Opens key: HKCU\software\classes\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}
Opens key: HKCU\software\classes\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}
Opens key: HKCU\software\classes\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}
Opens key: HKCU\software\classes\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}
Opens key: HKCU\software\classes\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}
Opens key: HKCU\software\classes\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid
Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\implemented categories
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\programmable
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\implemented categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
Opens key: HKLM\system\currentcontrolset\control\nls\codepage
Opens key: HKLM\software\wow6432node\microsoft\vba\monitors
Opens key: HKLM\software\microsoft\com3
Opens key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\treatas
Opens key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\treatas
Opens key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprochandler
Opens key: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprochandler
Opens key: HKCU\software\classes\appid\1aca077963eb842ac865c50dd866d52c.exe
Opens key: HKCR\appid\1aca077963eb842ac865c50dd866d52c.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}

Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\classes\aloahapopup.dialogs
Opens key: HKCR\aloahapopup.dialogs
Opens key: HKCU\software\policies\microsoft\windows\app management
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\app management
Opens key: HKLM\software\policies\microsoft\windows\app management
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKCU\software\classes\wow6432node\clsid\{acfb11f9-16bb-4fd7-9371-271f607c13d9}
Opens key: HKCR\wow6432node\clsid\{acfb11f9-16bb-4fd7-9371-271f607c13d9}
Opens key: HKCU\software\classes\clsid\{acfb11f9-16bb-4fd7-9371-271f607c13d9}
Opens key: HKCR\clsid\{acfb11f9-16bb-4fd7-9371-271f607c13d9}
Opens key: HKLM\software\wow6432node\microsoft\windows
Opens key: HKLM\software\wow6432node\microsoft\windows\html help
Opens key: HKLM\software\wow6432node\microsoft\windows\help
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[msvbvm60.dll]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[1aca077963eb842ac865c50dd866d52c]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKCR\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9\win32[]

Queries value: HKCR\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9\win32[]
Queries value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5[]
Queries value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags[]
Queries value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32[]
Queries value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir[]
Queries value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]
Queries value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[]
Queries value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[version]
Queries value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]
Queries value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]
Queries value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[]
Queries value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[version]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\progid[]
Queries value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}[]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[f810ecce]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp]
Sets/Creates value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5[]
Sets/Creates value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags[]
Sets/Creates value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32[]

Sets/Creates value: HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir[]
Sets/Creates value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]
Sets/Creates value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[]
Sets/Creates value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[version]
Sets/Creates value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]
Sets/Creates value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]
Sets/Creates value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[]
Sets/Creates value: HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[version]
Sets/Creates value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}[]
Sets/Creates value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\progid[]
Sets/Creates value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\localserver32[]
Sets/Creates value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\typelib[]
Sets/Creates value: HKCR\wow6432node\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\version[]
Sets/Creates value: HKCR\pdfsaver.remotecontrol[]
Sets/Creates value: HKCR\pdfsaver.remotecontrol\clsid[]
Sets/Creates value: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}[]
Sets/Creates value: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}[]
Sets/Creates value: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}[]
Sets/Creates value: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}[]
Sets/Creates value: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}[]
Sets/Creates value: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid[]
Value changes: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]
Value changes: HKCR\wow6432node\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]