Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 53, Task ID: 210

Task ID:	210
Risk Level:	1
Date Processed:	2016-04-28 12:53:09 (UTC)
Processing Time:	2.78 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\602364a4b81740b1e02627127600088a.exe"
Sample ID:	53
Type:	basic
Owner:	admin
Label:	602364a4b81740b1e02627127600088a
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	350856 bytes
MD5:	602364a4b81740b1e02627127600088a
SHA256:	acee4163520723c05718fe63d26f581c80503a1a54f7e70c340517a912b86665
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\602364a4b81740b1e02627127600088a.exe
["C:\windows\temp\602364a4b81740b1e02627127600088a.exe"]
Terminates process: C:\Windows\Temp\602364a4b81740b1e02627127600088a.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates semaphore: \Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?
602364A4B81740B1E02627127600088A.EXE

File System Events

Opens: C:\Windows\Prefetch\602364A4B81740B1E026271276000-616AA8D6.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\602364a4b81740b1e02627127600088a.exe
Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb
Opens: C:\Windows\SysWOW64\msvbvm60.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\imm32.dll

Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\clbcatq.dll
Opens: C:\Windows\SysWOW64\sxs.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\Windows\WINHELP.INI
Reads from: C:\Windows\Temp\602364a4b81740b1e02627127600088a.exe

Windows Registry Events

Creates key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}
Creates key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2
Creates key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags
Creates key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0
Creates key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32
Creates key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir
Creates key: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
Creates key: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib
Creates key: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
Creates key: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32
Creates key: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib
Creates key: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
Creates key: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib
Creates key: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
Creates key: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32
Creates key: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\progid
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\localserver32
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\typelib
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\version
Creates key: HKCR\aloahaprintercontrol.control
Creates key: HKCR\aloahaprintercontrol.control\clsid
Creates key: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}
Creates key: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\forward
Creates key: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}
Creates key: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\forward
Creates key: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}
Creates key: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-

3eee0fd115e0}\forward
Creates key: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}
Creates key: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\forward
Creates key: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\implemented categories
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\programmable
Creates key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\implemented categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
Deletes value: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\localserver32[threadingmodel]
Opens key: HKLM\software\microsoft\wow64
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\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
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\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

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\sorting\ids
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: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
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\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0
Opens key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0
Opens key: HKCU\software\classes\typelib
Opens key: HKCR\typelib
Opens key: HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}
Opens key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}
Opens key: HKLM\software\classes
Opens key: HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2
Opens key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2
Opens key: HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags
Opens key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags
Opens key: HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32
Opens key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32
Opens key: HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir
Opens key: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir
Opens key: HKCU\software\classes\wow6432node\interface
Opens key: HKCR\wow6432node\interface
Opens key: HKCU\software\classes\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
Opens key: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
Opens key: HKCU\software\classes\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib
Opens key: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib
Opens key: HKCU\software\classes\interface
Opens key: HKCR\interface
Opens key: HKCU\software\classes\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
Opens key: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
Opens key: HKCU\software\classes\interface\{590b6fce-d67f-4955-b9b9-

7c2e07745dd6}\proxystubclsid32
Opens key: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{590b6fce-d67f-4955-b9b9-
7c2e07745dd6}\typelib
Opens key: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib
Opens key: HKCU\software\classes\wow6432node\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}
Opens key: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
Opens key: HKCU\software\classes\wow6432node\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\typelib
Opens key: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\typelib
Opens key: HKCU\software\classes\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
Opens key: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
Opens key: HKCU\software\classes\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\proxystubclsid32
Opens key: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\typelib
Opens key: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\localserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\typelib
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\version
Opens key: HKCU\software\classes\aloahaprintercontrol.control
Opens key: HKCR\aloahaprintercontrol.control
Opens key: HKCU\software\classes\aloahaprintercontrol.control\clsid
Opens key: HKCU\software\classes\wow6432node\interface\{e8455db1-67d2-425f-80b9-
d6e4ed2304b2}
Opens key: HKCU\software\classes\wow6432node\interface\{e8455db1-67d2-425f-80b9-
d6e4ed2304b2}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{e8455db1-67d2-425f-80b9-
d6e4ed2304b2}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{e8455db1-67d2-425f-80b9-
d6e4ed2304b2}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{3782d58d-d973-4f9f-9820-
d4fb5a1dc4a3}
Opens key: HKCU\software\classes\wow6432node\interface\{3782d58d-d973-4f9f-9820-
d4fb5a1dc4a3}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{3782d58d-d973-4f9f-9820-
d4fb5a1dc4a3}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{3782d58d-d973-4f9f-9820-
d4fb5a1dc4a3}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{590b6fce-d67f-4955-b9b9-
7c2e07745dd6}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{0777556d-bd1d-4200-b408-
3eee0fd115e0}
Opens key: HKCU\software\classes\wow6432node\interface\{0777556d-bd1d-4200-b408-
3eee0fd115e0}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{0777556d-bd1d-4200-b408-
3eee0fd115e0}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{0777556d-bd1d-4200-b408-
3eee0fd115e0}\forward

Opens key: HKCU\software\classes\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}
Opens key: HKCU\software\classes\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\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\microsoft\com3
Opens key: HKLM\software\microsoft\windowsruntime\clsid
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0002e005-0000-0000-c000-000000000046}
Opens key: HKCR\activatableclasses\clsid
Opens key: HKCR\activatableclasses\clsid\{0002e005-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprochandler
Opens key: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\implemented categories
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\programmable
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\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\windowsruntime\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}
Opens key: HKCR\activatableclasses\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}
Opens key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\treatas
Opens key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-

2b7c067b6fdb}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprochandler
Opens key: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprochandler
Opens key: HKCU\software\classes\appid\602364a4b81740b1e02627127600088a.exe
Opens key: HKCR\appid\602364a4b81740b1e02627127600088a.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
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\software\wow6432node\microsoft\windows
Opens key: HKLM\software\wow6432node\microsoft\windows\html help
Opens key: HKLM\software\wow6432node\microsoft\windows\help
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: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
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\image file execution options\dllnxoptions[602364a4b81740b1e02627127600088a.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[602364a4b81740b1e02627127600088a]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
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\sorting\versions[000602xx]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
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: HKLM\software\microsoft\sqmclient\windows[ceipenable]
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\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2[]
Queries value: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags[]
Queries value: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32[]
Queries value: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir[]
Queries value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
Queries value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[]
Queries value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[version]
Queries value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
Queries value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
Queries value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[]
Queries value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[version]
Queries value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
Queries value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[]
Queries value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[version]
Queries value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
Queries value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]
Queries value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[]
Queries value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\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\rpc[idletimerwindow]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}[]
Queries value: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{0002e005-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
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: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}[]
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\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\ole[maxsxshashcount]
Queries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp]
Sets/Creates value: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2[]
Sets/Creates value: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags[]
Sets/Creates value: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32[]
Sets/Creates value: HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir[]
Sets/Creates value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
Sets/Creates value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[]
Sets/Creates value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[version]
Sets/Creates value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
Sets/Creates value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
Sets/Creates value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[]
Sets/Creates value: HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[version]
Sets/Creates value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
Sets/Creates value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[]
Sets/Creates value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[version]
Sets/Creates value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
Sets/Creates value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]
Sets/Creates value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[]
Sets/Creates value: HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[version]
Sets/Creates value: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}[]
Sets/Creates value: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\progid[]
Sets/Creates value: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\localserver32[]
Sets/Creates value: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\typelib[]
Sets/Creates value: HKCR\wow6432node\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\version[]
Sets/Creates value: HKCR\aloahaprintercontrol.control[]
Sets/Creates value: HKCR\aloahaprintercontrol.control\clsid[]
Sets/Creates value: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}[]
Sets/Creates value: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}[]
Sets/Creates value: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}[]

Sets/Creates value: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}[]
Sets/Creates value: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid[]
Value changes: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
Value changes: HKCR\wow6432node\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
Value changes: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
Value changes: HKCR\wow6432node\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]