Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 55, Task ID: 221

Task ID:	221
Risk Level:	3
Date Processed:	2016-04-28 12:53:12 (UTC)
Processing Time:	2.41 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\602bcc42064dbb0bcb1933b4247937fe.exe"
Sample ID:	55
Type:	basic
Owner:	admin
Label:	602bcc42064dbb0bcb1933b4247937fe
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	335872 bytes
MD5:	602bcc42064dbb0bcb1933b4247937fe
SHA256:	1cba995b5874702639b780fe754cb9d1f3f86238dbf00af062a1777221bb2a9c
Description:	None

Pattern Matching Results

3 Long sleep detected

Process/Thread Events

Creates process: C:\windows\temp\602bcc42064dbb0bcb1933b4247937fe.exe
["C:\windows\temp\602bcc42064dbb0bcb1933b4247937fe.exe"]
Terminates process: C:\Windows\Temp\602bcc42064dbb0bcb1933b4247937fe.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \KernelObjects\MaximumCommitCondition
Creates semaphore: \Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?
602BCC42064DBB0BCB1933B4247937FE.EXE

File System Events

Opens: C:\Windows\Prefetch\602BCC42064DBB0BCB1933B424793-FC85562C.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\602bcc42064dbb0bcb1933b4247937fe.exe
Opens: C:\windows\temp\602bcc42064dbb0bcb1933b4247937fe.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\WINHELP.INI
Opens: C:\Windows\SysWOW64\.HLP
Opens: C:\Windows\Help\.HLP
Reads from: C:\Windows\Temp\602bcc42064dbb0bcb1933b4247937fe.exe

Windows Registry Events

Creates key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}
Creates key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5
Creates key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags
Creates key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0
Creates key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32
Creates key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir
Creates key: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}
Creates key: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
Creates key: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}
Creates key: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
Creates key: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\progid
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\localserver32
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\typelib
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\version
Creates key: HKCR\aloahaflowchart64.engine64
Creates key: HKCR\aloahaflowchart64.engine64\clsid
Creates key: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}
Creates key: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\forward
Creates key: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}
Creates key: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\forward
Creates key: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}
Creates key: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\forward
Creates key: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}
Creates key: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\forward
Creates key: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}
Creates key: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-

8e104a921919}\proxystubclsid
Creates key: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid32
Creates key: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\forward
Creates key: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\implemented categories
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\programmable
Creates key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\implemented categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
Deletes value: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\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\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0
Opens key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0
Opens key: HKCU\software\classes\typelib
Opens key: HKCR\typelib
Opens key: HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}
Opens key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}
Opens key: HKLM\software\classes
Opens key: HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5
Opens key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5
Opens key: HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags
Opens key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags
Opens key: HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32
Opens key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32
Opens key: HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir
Opens key: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir
Opens key: HKCU\software\classes\wow6432node\interface
Opens key: HKCR\wow6432node\interface
Opens key: HKCU\software\classes\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}
Opens key: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}
Opens key: HKCU\software\classes\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
Opens key: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
Opens key: HKCU\software\classes\interface
Opens key: HKCR\interface
Opens key: HKCU\software\classes\interface\{d7a6a14f-7947-4899-be20-a019be861538}
Opens key: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}
Opens key: HKCU\software\classes\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
Opens key: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
Opens key: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\localserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\typelib
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\version
Opens key: HKCU\software\classes\aloahaflowchart64.engine64
Opens key: HKCR\aloahaflowchart64.engine64
Opens key: HKCU\software\classes\aloahaflowchart64.engine64\clsid
Opens key: HKCU\software\classes\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}
Opens key: HKCU\software\classes\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}
Opens key: HKCU\software\classes\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}
Opens key: HKCU\software\classes\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}
Opens key: HKCU\software\classes\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}
Opens key: HKCU\software\classes\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid
Opens key: HKCU\software\classes\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\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\{7a54054e-098c-460e-a45d-64f80a1b9754}\implemented categories
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\programmable
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-

64f80a1b9754}\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\{7a54054e-098c-460e-a45d-64f80a1b9754}
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\treatas
Opens key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\treatas
Opens key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprochandler
Opens key: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprochandler
Opens key: HKCU\software\classes\appid\602bcc42064dbb0bcb1933b4247937fe.exe
Opens key: HKCR\appid\602bcc42064dbb0bcb1933b4247937fe.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
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[602bcc42064dbb0bcb1933b4247937fe]
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\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5[]
Queries value: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags[]
Queries value: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32[]
Queries value: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir[]
Queries value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
Queries value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-
a019be861538}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-
a019be861538}\typelib[]
Queries value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-
a019be861538}\typelib[version]
Queries value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
Queries value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32[]
Queries value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[]
Queries value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\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\{7a54054e-098c-460e-a45d-64f80a1b9754}\progid[]
Queries value: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}[]
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[67e8c4d8]
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\software\wow6432node\microsoft\windows\html help[.hlp]
Sets/Creates value: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5[]
Sets/Creates value: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags[]
Sets/Creates value: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32[]
Sets/Creates value: HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir[]
Sets/Creates value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
Sets/Creates value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[]
Sets/Creates value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[version]
Sets/Creates value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
Sets/Creates value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32[]
Sets/Creates value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[]
Sets/Creates value: HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[version]
Sets/Creates value: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}[]
Sets/Creates value: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\progid[]
Sets/Creates value: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\localserver32[]
Sets/Creates value: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\typelib[]
Sets/Creates value: HKCR\wow6432node\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\version[]
Sets/Creates value: HKCR\aloahaflowchart64.engine64[]
Sets/Creates value: HKCR\aloahaflowchart64.engine64\clsid[]
Sets/Creates value: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}[]
Sets/Creates value: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}[]
Sets/Creates value: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}[]
Sets/Creates value: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{55af540b-13af-4de5-a975-5600b0589e59}\forward[]

Sets/Creates value: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}[]
Sets/Creates value: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}[]
Sets/Creates value: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid[]
Sets/Creates value: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid32[]
Sets/Creates value: HKCR\wow6432node\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\forward[]
Sets/Creates value: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid[]
Value changes: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
Value changes: HKCR\wow6432node\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32[]