

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 625, Task ID: 2445

Task ID: 2445
Risk Level: 4
Date Processed: 2016-02-22 05:31:06 (UTC)
Processing Time: 63.46 seconds
Virtual Environment: IntelliVM
Execution Arguments:
"c:\windows\temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeea8eb25c5920ef9b5d7026b.exe"

Sample ID: 625
Type: basic
Owner: admin
Label: cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeea8eb25c5920ef9b5d7026b
Date Added: 2016-02-22 05:26:50 (UTC)
File Type: PE32:win32:gui
File Size: 137728 bytes
MD5: 9b5e34f679602ae9dc1964e6279e2b82
SHA256: cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeea8eb25c5920ef9b5d7026b
Description: None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:
C:\windows\temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeea8eb25c5920ef9b5d7026b.exe
["C:\windows\temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeea8eb25c5920ef9b5d7026b.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens: C:\Windows\Prefetch\CBDD8E2ECCAA44F31B4217BD271F6-C6F96DB7.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeea8eb25c5920ef9b5d7026b.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\winmm.dll
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\winmmbase.dll
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\shlwapi.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\shell32.dll
Opens: C:\Windows\SysWOW64\comdlg32.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\nsi.dll
Opens: C:\Windows\SysWOW64\ws2_32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\mswsock.dll

Windows Registry Events

Opens key: HKLM\software\microsoft\wow64
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\currentversion\sidebyside\assemblystorageroots
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\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\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1c9e2bef
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
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\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b]
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[pageallocatorssystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivememtesting]
Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
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\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]

[illegible]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storiesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storiesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[transports]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[setup]
Queries value:

migration\providers\tcpip[winsock 2.0 provider id]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]