

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 625, Task ID: 2447

Task ID: 2447  
Risk Level: 4  
Date Processed: 2016-02-22 05:31:18 (UTC)  
Processing Time: 62.18 seconds  
Virtual Environment: IntelliVM  
Execution Arguments:  
"c:\windows\temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b.exe"

Sample ID: 625  
Type: basic  
Owner: admin  
Label: cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b  
Date Added: 2016-02-22 05:26:50 (UTC)  
File Type: PE32:win32:gui  
File Size: 137728 bytes  
MD5: 9b5e34f679602ae9dc1964e6279e2b82  
SHA256: cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b  
Description: None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:  
C:\windows\temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b.exe  
["C:\windows\temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b.exe" ]

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

## File System Events

Opens: C:\Windows\Prefetch\CBDD8E2ECAAA44F31B4217BD271F6-C6F96DB7.pf  
Opens: C:\Windows\System32  
Opens:  
C:\windows\temp\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b.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\System32\sechost.dll  
Opens: C:\windows\temp\WINMM.dll  
Opens: C:\Windows\System32\winmm.dll  
Opens: C:\Windows\System32\uxtheme.dll  
Opens: C:\Windows\System32\en-US\KernelBase.dll.mui  
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls  
Opens: C:\Windows\System32\mswsock.dll  
Opens: C:\Windows\System32\WSH\_TCPIP.DLL

## Windows Registry Events

Opens key: HKLM\system\currentcontrolset\control\session manager  
Opens key: HKLM\system\currentcontrolset\control\safeboot\option  
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll  
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers  
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers  
Opens key: HKCU\  
Opens key: HKCU\control panel\desktop\mui\cached\machinelanguageconfiguration  
Opens key: HKLM\software\policies\microsoft\mui\settings  
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\mui\cached  
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside  
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions  
Opens key: HKLM\system\currentcontrolset\control\error message instrument\  
Opens key: HKLM\system\currentcontrolset\control\error message instrument  
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize  
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32  
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility  
Opens key: HKLM\  
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows  
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics  
Opens key: HKLM\software\microsoft\ole

Opens key: HKLM\software\microsoft\ole\tracing  
Opens key: HKLM\software\microsoft\oleaut  
Opens key: HKLM\system\currentcontrolset\control\cmf\config  
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr  
Opens key: HKLM\software\policies\microsoft\sqlclient\windows  
Opens key: HKLM\software\microsoft\sqlclient\windows  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters  
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale  
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
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\00000019  
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\protocol\_catalog9\catalog\_entries\000000000011  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000012  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000013  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000014  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000015  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000016  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000017  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000018  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\0000000c  
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\tcpip6\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\psched  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip  
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]

Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
Queries value: HKCU\control panel\desktop[preferreduilanguages]  
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]  
Queries value:  
HKLM\software\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\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\compatibility32[cbdd8e2eccaa44f31b4217bd271f665becb2b9ffea8eb25c5920ef9b5d7026b]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]  
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]  
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\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]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000011[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000012[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000013[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000014[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000015[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000016[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000017[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000018[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[librarypath]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[displaystring]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerid]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[addressfamily]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[enabled]

[illegible]

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[storserviceclassinfo]  
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\winsock2\parameters[ws2\_32spincount]  
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]  
Queries value:  
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\psched[winsock 2.0 provider id]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
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]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]