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\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeaa8eb25c5920ef9b5d7026b.exe"

Sample ID: 625 Type: basic Owner: admin

Label: cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeaa8eb25c5920ef9b5d7026b

Date Added: 2016-02-22 05:26:50 (UTC)

File Type: PE32:win32:gui File Size: 137728 bytes

MD5: 9b5e34f679602ae9dc1964e6279e2b82

SHA256: cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeaa8eb25c5920ef9b5d7026b

Description: None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:

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\cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeaa8eb25c5920ef9b5d7026b.exe

Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-

controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954

 $Opens: C: \windows\winSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comct132.dll$

C:\Windows\SysWOW64\combase.dll Opens: Opens: C:\Windows\SysWOW64\sechost.dll C:\Windows\SysWOW64\winmmbase.dll Opens: Opens: C:\Windows\SysWOW64\SHCore.dll Opens: C:\Windows\SysWOW64\gdi32.dll C:\Windows\SysWOW64\user32.dll Opens: Opens: C:\Windows\SysWOW64\msvcrt.dll Opens: C:\Windows\SysWOW64\shlwapi.dll

Opens: C:\Windows\SysWOW64\bexpyttprimitives.dll

Opens: C:\Windows\SysWOW64\cryptbase.dll C:\Windows\SysWOW64\sspicli.dll Opens: Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: C:\Windows\SysWOW64\advapi32.dll C:\Windows\SysWOW64\shell32.dll Opens: Opens: C:\Windows\SysWOW64\comdlg32.dll Opens: C:\Windows\SysWOW64\ole32.dll C:\Windows\SysWOW64\oleaut32.dll Opens: Opens: C:\Windows\SysWOW64\nsi.dll C:\Windows\SysWOW64\ws2_32.dll Opens: 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 kev:
                       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
                       HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
 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:
                       Opens key:
                       HKLM\software\wow6432node\policies\microsoft\mui\settings
                       {\tt HKLM \backslash software \backslash policies \backslash microsoft \backslash mui \backslash settings}
 Opens key:
 Opens key:
                       HKCU\
 Opens key:
                       HKCU\control panel\desktop\muicached\machinelanguageconfiguration
                       HKLM\svstem\currentcontrolset\control\mui\settings\languageconfiguration
 Opens kev:
 Opens key:
                       HKCU\software\policies\microsoft\control panel\desktop
 Opens key:
                       HKCU\control panel\desktop\languageconfiguration
                       HKCU\control panel\desktop
 Opens key:
 Opens key:
                       HKCU\control panel\desktop\muicached
 Opens key:
                       HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
                       HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens kev:
 Opens key:
                       HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
 Opens key:
                       HKCU\software\microsoft\windows nt\currentversion\appcompatflags
                       HKLM\software\microsoft\windows
 Opens key:
nt\currentversion\appcompatflags\disable8and16bitmitigation
 Opens key:
                       HKLM\system\currentcontrolset\control\session manager
 Opens key:
Opens key:
                       HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
                       HKLM\software\wow6432node\microsoft\windows
 Opens key:
nt\currentversion\compatibility32
                      HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
 Opens key:
compatibility
 Opens key:
                      HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
 Opens key:
 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
                       HKLM\software\microsoft\ole
 Opens key:
 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 kev:
                       HKLM\software\microsoft\samclient\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:
                       Opens kev:
                       HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus appid\_catalog \setminus 1c9e2bef
 Opens kev:
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 kev:
Opens kev:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007

Opens key:

Opens kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010

Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014 Opens kev: 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\000000000000 Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004 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] HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback] HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries value: Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\enus[alternatecodepage] HKCU\control panel\desktop[preferreduilanguages] Queries value: Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]]$ HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value: HKCU\software\microsoft\windows Oueries value: nt\currentversion\appcompatflags[showdebuginfo] Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] HKLM\software\microsoft\windows Queries value: nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[cbdd8e2eccaa44f31b4217bd271f665becb2b9ffeaa8eb25c5920ef9b5d7026b] HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\windows[loadappinit_dlls] HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Queries value: Oueries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKLM\software\microsoft\ole[aggressivemtatesting] HKLM\software\microsoft\sqmclient\windows[ceipenable] Oueries value: HKLM\system\currentcontrolset\control\cmf\config[system] Oueries value: Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]

Oueries value:

Queries value.

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries 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] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries 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\00000000001[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo] Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000004 [library path] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Queries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_lember \namespace_le$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 [storesservice class info] \ Oueries \ value:$
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]

 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters [ws2_32numhandle buckets]$
- Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 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:
- Queries value:
- $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} is a parameter \end{tabular} winsock \cite{local_ham} used \cite{local_ham} and \cite{local_ham} used \cite{local_ham} u$