Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 626, Task ID: 2449

Task ID: 2449 Risk Level: 5

Date Processed: 2016-02-22 05:31:25 (UTC)

Processing Time: 61.25 seconds
Virtual Environment: IntelliVM

Execution Arguments:

"c:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe"

Sample ID: 626 Type: basic Owner: admin

Label: b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5

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

File Type: PE32:win32:gui File Size: 393212 bytes

MD5: ba04839db97a1b934cd9e470795ccf51

SHA256: b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5

Description: None

Pattern Matching Results

5 Abnormal sleep detected

5 Possible injector

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process

C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe ["C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens: C:\Windows\Prefetch\B3AF5BCCF7891B0251AAA73F063F1-4CD469AF.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dl1
Opens: C:\Windows\SysWOW64

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

Opens:

Opens:

C:\Windows\Temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe

Opens: C:\Windows\SysWOW64\ntdll.dll C:\Windows\SysWOW64\kernel32.dll Opens: Opens: C:\Windows\SysWOW64\KernelBase.dll Opens: C:\Windows\apppatch\sysmain.sdb C:\Windows\SysWOW64\version.dll Opens: Opens: C:\Windows\SysWOW64\wsock32.dll Opens: C:\Windows\SysWOW64\winmm.dll Opens: C:\Windows\SysWOW64\atl.dll Opens: C:\Windows\SysWOW64\wtsapi32.dll Opens: C:\Windows\SysWOW64\sechost.dll C:\Windows\SysWOW64\winmmbase.dll Opens: 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 C:\Windows\SysWOW64\sspicli.dll Opens: Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: C:\Windows\SysWOW64\advapi32.dll Opens: C:\Windows\SysWOW64\combase.dll C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\SysWOW64\iertutil.dll Opens: Opens: C:\Windows\SysWOW64\wininet.dll C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\nsi.dll Opens: C:\Windows\SysWOW64\ws2_32.dll Opens: C:\Windows\SysWOW64\psapi.dll Opens: C:\Windows\SysWOW64\shlwapi.dll Opens: C:\Windows\SysWOW64\shell32.dll Opens:

C:\Windows\SysWOW64\urlmon.dll

Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll

Opens key:

Windows Registry Events

Opens key: HKLM\software\microsoft\wow64 Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key: ${\it HKLM \ } system \verb|\ current control \ safe boot \verb|\ option| \\$ Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: 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 HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: 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 HKCU\ Opens key: Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration HKCU\software\policies\microsoft\control panel\desktop Opens key: ${\it HKCU} \ control\ panel\ desktop\ language configuration$ Opens key: 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 kev: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation HKLM\system\currentcontrolset\control\session manager Opens key: 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 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows$ Opens key: nt\currentversion\compatibility32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility Opens key: Opens kev: 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 HKLM\software\wow6432node\microsoft\ole\tracing Opens key: Opens key: HKLM\software\microsoft\ole\tracing HKLM\software\wow6432node\microsoft\oleaut Opens key: Opens key: HKCU\software\borland\locales Opens key: HKCU\software\borland\delphi\locales Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale HKLM\software\policies\microsoft\sqmclient\windows Opens kev: Opens key: HKLM\software\microsoft\sqmclient\windows Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: $\label{lem:hklm} \verb+ HKLM \system \current control \end{tabular} ids$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\31f8160b HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol_catalog 9 \setminus 00000005$ Opens key: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog_entries$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens kev:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 000000000010) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (catal$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

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 key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006

HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value: Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Queries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Queries value:

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

Oueries value: HKCU\control panel\desktop[preferreduilanguages]

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side [preferex ternal manifest]$

HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value:

HKCU\software\microsoft\windows Queries value:

nt\currentversion\appcompatflags[showdebuginfo]

HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value:

options\dllnxoptions[usefilter]

HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value: options\dllnxoptions[b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da3499cdd80c1fcc5.exe]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Oueries value:

 $nt \verb|\currentversion| compatibility 32[b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5]| above the following the following$

HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\windows[loadappinit dlls]

HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Oueries value:

HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Queries value: Oueries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

HKLM\software\microsoft\ole[aggressivemtatesting] Oueries value:

HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value:

Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]

HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] Oueries 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]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries] Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem] Oueries value:

Oueries value:

Oueries 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\000000000007[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]
 Queries 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\000000000001[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
- 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]
 Oueries 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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[addressfamily] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries 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\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names \pace_catalog 5 \catalog_entries \names \names \pace_catalog 5 \catalog_entries \names \$

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
 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\00000000005[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
 Queries value:
- $\label{lem:hklmsystem} Hklm\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]\\ Queries\ value:$
- 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 numhandle buckets]$