Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 75, Task ID: 301

Task ID:	301
Risk Level:	1
Date Processed:	2016-04-28 12:55:39 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ca3224d4e0889ee8fb5cd5f181f77120.exe"

Sample ID:	75
Type:	basic
Owner:	admin
Label:	ca3224d4e0889ee8fb5cd5f181f77120
Date Added:	2016-04-28 12:44:57 (UTC)
File Type:	PE32:win32:gui
File Size:	425984 bytes
MD5:	ca3224d4e0889ee8fb5cd5f181f77120
SHA256:	9c334211422ddf7f0895acd1061733b2d270b7b909314703d7f254bffb16f9fa
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\windows\temp\ca3224d4e0889ee8fb5cd5f181f77120.exe ["C:\windows\temp\ca3224d4e0889ee8fb5cd5f181f77120.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?CA3224D4E0889EE8FB5CD5F181F77120.EXE

File System Events

Opens:	C:\Windows\Prefetch\CA3224D4E0889EE8FB5CD5F181F77-4B0C0707.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\ca3224d4e0889ee8fb5cd5f181f77120.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\ca3224d4e0889ee8fb5cd5f181f77120.exe.Local\
  Opens:                   C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
  Opens:                   C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:                   C:\Windows\WindowsShell.Manifest
  Opens:                   C:\Windows\SysWOW64\VB6DE.DLL
  Opens:                   C:\Windows\Fonts\sserife.fon
  Opens:                   C:\windows\temp\dwmapi.dll
  Opens:                   C:\Windows\SysWOW64\dwmapi.dll
  Opens:                   C:\Windows\SysWOW64\en-US\user32.dll.mui
  Opens:                   C:\Windows\SysWOW64\asycfilt.dll
  Opens:                   C:\Windows\Fonts\calibriz.ttf
  Opens:                   C:\Windows\Fonts\verdana.ttf
  Opens:                   C:\Windows\Fonts\calibrib.ttf
  Opens:                   C:\windows\temp\VERSION.DLL
  Opens:                   C:\Windows\SysWOW64\version.dll
  Opens:                   C:\Windows\Temp\ca3224d4e0889ee8fb5cd5f181f77120.exe
  Opens:                   C:\Windows\Fonts\StaticCache.dat
  Opens:                   C:\Windows\SysWOW64\kernel32.dll
  Opens:                   C:\Windows\SysWOW64\ole32.dll
  Reads from:              C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
  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:                 HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                 HKLM\software\wow6432node\microsoft\vba\monitors
  Opens key:                 HKCU\software\classes\
  Opens key:                 HKLM\software\microsoft\com3
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{3cd9dba0-6409-4c4d-a3cd-
742c7e99f176}
  Opens key:                 HKCR\wow6432node\clsid\{3cd9dba0-6409-4c4d-a3cd-742c7e99f176}
  Opens key:                 HKCU\software\classes\clsid\{3cd9dba0-6409-4c4d-a3cd-742c7e99f176}
  Opens key:                 HKCR\clsid\{3cd9dba0-6409-4c4d-a3cd-742c7e99f176}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{a57f28d5-96b7-46ce-859b-
128ab69b3234}
  Opens key:                 HKCR\wow6432node\clsid\{a57f28d5-96b7-46ce-859b-128ab69b3234}
  Opens key:                 HKCU\software\classes\clsid\{a57f28d5-96b7-46ce-859b-128ab69b3234}
  Opens key:                 HKCR\clsid\{a57f28d5-96b7-46ce-859b-128ab69b3234}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cc4a6592-195d-4ae0-93ac-
604557c39ff7}
  Opens key:                 HKCR\wow6432node\clsid\{cc4a6592-195d-4ae0-93ac-604557c39ff7}
  Opens key:                 HKCU\software\classes\clsid\{cc4a6592-195d-4ae0-93ac-604557c39ff7}
  Opens key:                 HKCR\clsid\{cc4a6592-195d-4ae0-93ac-604557c39ff7}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                 HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\ca3224d4e0889ee8fb5cd5f181f77120.exe
  Opens key:                 HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:                 HKLM\software\wow6432node\microsoft\ctf\
  Opens key:                 HKLM\software\wow6432node\microsoft\ctf\knownclasses
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
  Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms sans serif
  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[ca3224d4e0889ee8fb5cd5f181f77120]
  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:              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:              HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[de-de]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[de-de]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:              HKLM\software\microsoft\windows
```

```
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:               HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:               HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
```