Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 615, Task ID: 2408

Task ID:	2408
Risk Level:	2
Date Processed:	2016-02-22 05:26:53 (UTC)
Processing Time:	26.66 seconds
Virtual Environment:	IntelliVM

Execution Arguments:
"c:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe"

Sample ID:	615
Type:	basic
Owner:	admin
Label:	8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96
Date Added:	2016-02-22 05:26:48 (UTC)
File Type:	PE32:win32:gui:.net
File Size:	50688 bytes
MD5:	d3109c83e07dd5d7fe032dc80c581d08
SHA256:	8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96
Description:	None

Pattern Matching Results

2 .NET compiled executable

Process/Thread Events

Creates process:
C:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
["C:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe"]
Terminates process:
C:\Windows\Temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens: C:\Windows\Prefetch\8995535721EBEAF6983C6CECF3182-53289CA2.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\SysWOW64\mscoree.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\MSCOREE.DLL.local
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727
Opens: C:\Windows\Microsoft.NET\Framework\Upgrades.2.0.50727\
Opens: C:\Windows\SysWOW64\imm32.dll
Opens:
C:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.config
Opens:
C:\Windows\Temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
Opens: C:\Windows\Microsoft.NET\Framework\v4.0.30319\
Opens: C:\Windows\SysWOW64\MUI\0409\mscorees.dll
Opens: C:\Windows\SysWOW64\mscorrc.dll
Opens: C:\Windows\SysWOW64\mscorrc.dll.DLL
Opens: C:\Windows\SYSTEM32\mscorrc.dll

Opens: C:\Windows\SYSTEM32\mscorrc.dll.DLL
Opens: C:\windows\temp\mscorrc.dll
Opens: C:\Windows\system\mscorrc.dll
Opens: C:\Windows\mscorrc.dll
Opens: C:\Windows\SysWOW64\Wbem\mscorrc.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\mscorrc.dll
Opens: C:\Windows\Microsoft.NET\Framework\v4.0.40305\
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.Local\
Opens: C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac
Opens: C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac\comctl32.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\nls\sorting\versions
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\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\v2.0
Opens key: HKLM\software\wow6432node\microsoft\.netframework
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\upgrades
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\standards
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch
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: HKCU\software\microsoft\.netframework\policy\standards
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v4.0.30319
Opens key: HKCU\software\microsoft\.netframework\policy\upgrades
Opens key: HKCU\software\microsoft\.netframework
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
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\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\windows\currentversion\sidebyside\assemblystorageroots
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\nls\sorting\versions[]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
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\software\wow6432node\microsoft\.netframework[installroot]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[noguifromshim]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
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\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]