Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 190, Task ID: 761

Task ID:	761
Risk Level:	4
Date Processed:	2016-04-28 13:08:15 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\592ec975d7f4ee422e9c4a1f5d08497c.exe"
Sample ID:	190
Type:	basic
Owner:	admin
Label:	592ec975d7f4ee422e9c4a1f5d08497c
Date Added:	2016-04-28 12:45:09 (UTC)
File Type:	PE32:win32:gui
File Size:	293848 bytes
MD5:	592ec975d7f4ee422e9c4a1f5d08497c
SHA256:	6414f33b7eb649d1e7b1d18ac5b3f8aacb8dc8028c068bb7b031b66cd3d62b80
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\592ec975d7f4ee422e9c4a1f5d08497c.exe
["C:\windows\temp\592ec975d7f4ee422e9c4a1f5d08497c.exe"]

File System Events

Opens: C:\Windows\Prefetch\592EC975D7F4EE422E9C4A1F5D084-B295ACF9.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\WINMM.dll
Opens: C:\Windows\SysWOW64\winmm.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\CardBase.dll
Opens: C:\Windows\SysWOW64\CardBase.dll
Opens: C:\Windows\system\CardBase.dll
Opens: C:\Windows\CardBase.dll
Opens: C:\Windows\SysWOW64\Wbem\CardBase.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\CardBase.dll

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\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
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\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]