Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 115, Task ID: 461

Task ID:	461
Risk Level:	8
Date Processed:	2016-04-28 12:59:31 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\71ee06c836c06dc9070744db6a072a1e.exe"
Sample ID:	115
Type:	basic
Owner:	admin
Label:	71ee06c836c06dc9070744db6a072a1e
Date Added:	2016-04-28 12:45:02 (UTC)
File Type:	PE32:win32:gui
File Size:	175880 bytes
MD5:	71ee06c836c06dc9070744db6a072a1e
SHA256:	765a50799e74731fef1ad77366e68ff8efdef348a35934fa0ecf94b2c0a3f2b3
Description:	None

Pattern Matching Results

8 Contains suspicious Microsoft certificate

Process/Thread Events

Creates process: C:\windows\temp\71ee06c836c06dc9070744db6a072a1e.exe ["C:\windows\temp\71ee06c836c06dc9070744db6a072a1e.exe"]

File System Events

Opens: C:\Windows\Prefetch\71EE06C836C06DC9070744DB6A072-DCB7B45C.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\Secur32.dll
Opens: C:\Windows\SysWOW64\secur32.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\CtrlFactory.dll
Opens: C:\Windows\SysWOW64\CtrlFactory.dll
Opens: C:\Windows\system\CtrlFactory.dll
Opens: C:\Windows\CtrlFactory.dll
Opens: C:\Windows\SysWOW64\Wbem\CtrlFactory.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\CtrlFactory.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\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
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]