Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	460
Risk Level:	8
Date Processed:	2016-04-28 12:59:29 (UTC)
Processing Time:	61.11 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\System32
Opens:	C:\windows\temp\Secur32.dll
Opens:	C:\Windows\System32\secur32.dll
Opens:	C:\windows\temp\SSPICLI.DLL
Opens:	C:\Windows\System32\sspicli.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\CtrlFactory.dll
Opens:	C:\Windows\system32\CtrlFactory.dll
Opens:	C:\Windows\system\CtrlFactory.dll
Opens:	C:\Windows\CtrlFactory.dll
Opens:	C:\Windows\System32\Wbem\CtrlFactory.dll
Opens:	C:\Windows\System32\WindowsPowerShell\v1.0\CtrlFactory.dll

Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
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\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\softare\policies\microsoft\mui\settings
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\microsoft\windows\currentversion\sidebyside

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: HKCU\control panel\desktop[preferreduilanguages]
    Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
    Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]