Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 166, Task ID: 665

Task ID:	665
Risk Level:	5
Date Processed:	2016-04-28 13:05:21 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0c05a151bc2c66fd6112346d6c7e0e06.exe"
Sample ID:	166
Type:	basic
Owner:	admin
Label:	0c05a151bc2c66fd6112346d6c7e0e06
Date Added:	2016-04-28 12:45:07 (UTC)
File Type:	PE32:win32:gui
File Size:	108544 bytes
MD5:	0c05a151bc2c66fd6112346d6c7e0e06
SHA256:	3a4d8bd4c397c5b06bc8abf72d1cf547630b92336ff59e7001574a201a802531
Description:	None

Pattern Matching Results

2 PE: Nonstandard section
4 Checks whether debugger is present
5 PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\windows\temp\0c05a151bc2c66fd6112346d6c7e0e06.exe
["C:\windows\temp\0c05a151bc2c66fd6112346d6c7e0e06.exe"]

File System Events

Opens:	C:\Windows\Prefetch\0C05A151BC2C66FD6112346D6C7E0-3C4C0D1B.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\libvlc.dll
Opens:	C:\Windows\SysWOW64\libvlc.dll
Opens:	C:\Windows\system\libvlc.dll
Opens:	C:\Windows\libvlc.dll
Opens:	C:\Windows\SysWOW64\Wbem\libvlc.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\libvlc.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
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]