Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 38, Task ID: 152

Task ID:	152
Risk Level:	1
Date Processed:	2016-04-28 12:51:02 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\785c8b71605e40c35d546b1d9ab1681f.exe"
Sample ID:	38
Type:	basic
Owner:	admin
Label:	785c8b71605e40c35d546b1d9ab1681f
Date Added:	2016-04-28 12:44:53 (UTC)
File Type:	PE32:win32:gui
File Size:	201688 bytes
MD5:	785c8b71605e40c35d546b1d9ab1681f
SHA256:	fb10cec0b3ad436990c160e95d0c35b995255c736c8283822c410e59821a2bb4
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\785c8b71605e40c35d546b1d9ab1681f.exe ["C:\windows\temp\785c8b71605e40c35d546b1d9ab1681f.exe"]

File System Events

Opens: C:\Windows\Prefetch\785C8B71605E40C35D546B1D9AB16-4CC9BAA0.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\k2.dll
Opens: C:\Windows\SysWOW64\k2.dll
Opens: C:\Windows\system\k2.dll
Opens: C:\Windows\k2.dll
Opens: C:\Windows\SysWOW64\Wbem\k2.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\k2.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]