Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 33, Task ID: 132

Task ID:	132
Risk Level:	1
Date Processed:	2016-04-28 12:50:33 (UTC)
Processing Time:	3.41 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\b234b5941bf3b1324dc120aa27e2edc6.exe"
Sample ID:	33
Type:	basic
Owner:	admin
Label:	b234b5941bf3b1324dc120aa27e2edc6
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	49880 bytes
MD5:	b234b5941bf3b1324dc120aa27e2edc6
SHA256:	f9fc3ee63820b541be573d2a20c2c49647e4f99569d87a57feb9697fc5e1f0d9
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\b234b5941bf3b1324dc120aa27e2edc6.exe ["C:\windows\temp\b234b5941bf3b1324dc120aa27e2edc6.exe"]
Terminates process: C:\Windows\Temp\b234b5941bf3b1324dc120aa27e2edc6.exe

File System Events

Opens: C:\Windows\Prefetch\B234B5941BF3B1324DC120AA27E2E-A3F5B4DD.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

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\sorting\versions
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\sorting\versions[]