Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 18, Task ID: 72

Task ID:	72
Risk Level:	1
Date Processed:	2016-04-28 12:48:41 (UTC)
Processing Time:	62.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7a81151e615b04638ac056c428c42423.exe"
Sample ID:	18
Type:	basic
Owner:	admin
Label:	7a81151e615b04638ac056c428c42423
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	915472 bytes
MD5:	7a81151e615b04638ac056c428c42423
SHA256:	a07c92d0dc9a27a149cc905ba41160b8d8550b19934e181a082e8a1118e5dcc3
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\7a81151e615b04638ac056c428c42423.exe ["C:\windows\temp\7a81151e615b04638ac056c428c42423.exe"]

File System Events

Opens: C:\Windows\Prefetch\7A81151E615B04638AC056C428C42-C717D496.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\vcl100.bpl
Opens: C:\Windows\SysWOW64\vcl100.bpl
Opens: C:\Windows\system\vcl100.bpl
Opens: C:\Windows\vcl100.bpl
Opens: C:\Windows\SysWOW64\Wbem\vcl100.bpl
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\vcl100.bpl

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]