Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	791
Risk Level:	4
Date Processed:	2016-04-28 13:09:33 (UTC)
Processing Time:	2.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\52fd1e3fbd2bc9460fda9703084b404f.exe"

Sample ID:	198
Type:	basic
Owner:	admin
Label:	52fd1e3fbd2bc9460fda9703084b404f
Date Added:	2016-04-28 12:45:10 (UTC)
File Type:	PE32:win32:gui
File Size:	7680 bytes
MD5:	52fd1e3fbd2bc9460fda9703084b404f
SHA256:	155f5f74f8f362759ad305ff48055f199e23e64519bad1f5e39d50d791f7942f
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\52fd1e3fbd2bc9460fda9703084b404f.exe ["c:\windows\temp\52fd1e3fbd2bc9460fda9703084b404f.exe"]
Terminates process: C:\WINDOWS\Temp\52fd1e3fbd2bc9460fda9703084b404f.exe

File System Events

Opens: C:\WINDOWS\Prefetch\52FD1E3FBD2BC9460FDA9703084B4-05570FCE.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e\msvcr90.dll
Opens: C:\
Opens: C:\WINDOWS
Opens: C:\WINDOWS\system32
Opens: C:\WINDOWS\system32\wbem
Opens: C:\WINDOWS\Temp

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\52fd1e3fbd2bc9460fda9703084b404f.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcr90.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

```
options\kernel32.dll
  Opens key:              HKCU\
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:              HKCU\control panel\desktop
  Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:          HKCU\control panel\desktop[multiuilanguageid]
```