Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	373
Risk Level:	1
Date Processed:	2016-04-28 12:57:14 (UTC)
Processing Time:	3.46 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\2d227eb0d416daad9b011fcc9a9062e9.exe"

Sample ID:	93
Type:	basic
Owner:	admin
Label:	2d227eb0d416daad9b011fcc9a9062e9
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	61440 bytes
MD5:	2d227eb0d416daad9b011fcc9a9062e9
SHA256:	f61090e9f71976a5043a7a7cfec8a577c8555d997727548d7595b162a10c5ae4
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\windows\temp\2d227eb0d416daad9b011fcc9a9062e9.exe ["C:\windows\temp\2d227eb0d416daad9b011fcc9a9062e9.exe"]
Terminates process:	C:\Windows\Temp\2d227eb0d416daad9b011fcc9a9062e9.exe

File System Events

Opens:	C:\Windows\Prefetch\2D227EB0D416DAAD9B011FCC9A906-003B8A13.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[]