Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	725
Risk Level:	5
Date Processed:	2016-04-28 13:07:37 (UTC)
Processing Time:	61.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\25f424cb9894dd2808f2c387eac9ccc3.exe"

Sample ID:	181
Type:	basic
Owner:	admin
Label:	25f424cb9894dd2808f2c387eac9ccc3
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	851264 bytes
MD5:	25f424cb9894dd2808f2c387eac9ccc3
SHA256:	eb1d325f1225109b2873593b8d21ca300bd8a58209442c998d26abef3fce00ac
Description:	None

Pattern Matching Results

5 PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\25f424cb9894dd2808f2c387eac9ccc3.exe ["C:\windows\temp\25f424cb9894dd2808f2c387eac9ccc3.exe"]

File System Events

Opens:	C:\Windows\Prefetch\25F424CB9894DD2808F2C387EAC9C-E7BCF6C7.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\rtl120.bpl
Opens:	C:\Windows\SysWOW64\rtl120.bpl
Opens:	C:\Windows\system\rtl120.bpl
Opens:	C:\Windows\rtl120.bpl
Opens:	C:\Windows\SysWOW64\Wbem\rtl120.bpl
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rtl120.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]
```