Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 258, Task ID: 1033

Task ID:	1033
Risk Level:	1
Date Processed:	2016-04-28 13:16:01 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\be53d60a10e36a218bd098ed01d8d075.exe"

Sample ID:	258
Type:	basic
Owner:	admin
Label:	be53d60a10e36a218bd098ed01d8d075
Date Added:	2016-04-28 12:45:16 (UTC)
File Type:	PE32:win32:gui
File Size:	180520 bytes
MD5:	be53d60a10e36a218bd098ed01d8d075
SHA256:	5dbbf8c63a7ff2a8f668db23946c1e9a14e833a2224a36e5a57b937530eb239d
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\be53d60a10e36a218bd098ed01d8d075.exe ["C:\windows\temp\be53d60a10e36a218bd098ed01d8d075.exe"]

File System Events

Opens:	C:\Windows\Prefetch\BE53D60A10E36A218BD098ED01D8D-7F831626.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\rtl160.bpl
Opens:	C:\Windows\SysWOW64\rtl160.bpl
Opens:	C:\Windows\system\rtl160.bpl
Opens:	C:\Windows\rtl160.bpl
Opens:	C:\Windows\SysWOW64\Wbem\rtl160.bpl
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rtl160.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]
```