Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 51, Task ID: 205

Task ID:	205
Risk Level:	4
Date Processed:	2016-04-28 12:52:31 (UTC)
Processing Time:	61.35 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6042f2e158929323e1f7ef4aeadd6d82.exe"
Sample ID:	51
Type:	basic
Owner:	admin
Label:	6042f2e158929323e1f7ef4aeadd6d82
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	260568 bytes
MD5:	6042f2e158929323e1f7ef4aeadd6d82
SHA256:	5de9c26d1c7ec9a51801ec4db737a73c96fd44235d35f5f2e82bb35d3917f143
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\6042f2e158929323e1f7ef4aeadd6d82.exe ["C:\windows\temp\6042f2e158929323e1f7ef4aeadd6d82.exe"]

File System Events

Opens: C:\Windows\Prefetch\6042F2E158929323E1F7EF4AEADD6-4E2266EC.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\CardBase.dll
Opens: C:\Windows\SysWOW64\CardBase.dll
Opens: C:\Windows\system\CardBase.dll
Opens: C:\Windows\CardBase.dll
Opens: C:\Windows\SysWOW64\Wbem\CardBase.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\CardBase.dll

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\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\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]