Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 107, Task ID: 429

Task ID:	429
Risk Level:	4
Date Processed:	2016-04-28 12:58:47 (UTC)
Processing Time:	61.24 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\89412b3b78ebee72a87c2bbd56f0b0c4.exe"
Sample ID:	107
Type:	basic
Owner:	admin
Label:	89412b3b78ebee72a87c2bbd56f0b0c4
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	17304 bytes
MD5:	89412b3b78ebee72a87c2bbd56f0b0c4
SHA256:	4c60ae40c0e3dceb2b98e4b7cf7caab42282eaf74211c7cb53972ad99d8fbf3d
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\89412b3b78ebee72a87c2bbd56f0b0c4.exe ["C:\windows\temp\89412b3b78ebee72a87c2bbd56f0b0c4.exe"]

File System Events

Opens: C:\Windows\Prefetch\89412B3B78EBEE72A87C2BBD56F0B-ED66CBDF.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\xul.dll
Opens: C:\Windows\SysWOW64\xul.dll
Opens: C:\Windows\system\xul.dll
Opens: C:\Windows\xul.dll
Opens: C:\Windows\SysWOW64\Wbem\xul.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\xul.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]