Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 111, Task ID: 445

Task ID:	445
Risk Level:	4
Date Processed:	2016-04-28 12:59:20 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\4a7749dcc24c8c7d145a39e8e132b17c.exe"
Sample ID:	111
Type:	basic
Owner:	admin
Label:	4a7749dcc24c8c7d145a39e8e132b17c
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	91608 bytes
MD5:	4a7749dcc24c8c7d145a39e8e132b17c
SHA256:	4bd9267536ce850dd8dee4ff1a8c0ff0253170043c1c3295200fc445eb3f2cb2
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\4a7749dcc24c8c7d145a39e8e132b17c.exe ["C:\windows\temp\4a7749dcc24c8c7d145a39e8e132b17c.exe"]

File System Events

Opens: C:\Windows\Prefetch\4A7749DCC24C8C7D145A39E8E132B-0ACDB6E5.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\MfcExt.dll
Opens: C:\Windows\SysWOW64\MfcExt.dll
Opens: C:\Windows\system\MfcExt.dll
Opens: C:\Windows\MfcExt.dll
Opens: C:\Windows\SysWOW64\Wbem\MfcExt.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\MfcExt.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]