Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 91, Task ID: 365

Task ID:	365
Risk Level:	4
Date Processed:	2016-04-28 12:57:14 (UTC)
Processing Time:	61.28 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ae329ad95f7a6c49f8dacb3358aa3230.exe"
Sample ID:	91
Type:	basic
Owner:	admin
Label:	ae329ad95f7a6c49f8dacb3358aa3230
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	510936 bytes
MD5:	ae329ad95f7a6c49f8dacb3358aa3230
SHA256:	70303305b8b0e9923c678abc028376df4be69c7d299b9517816215d34b9f0776
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\ae329ad95f7a6c49f8dacb3358aa3230.exe ["C:\windows\temp\ae329ad95f7a6c49f8dacb3358aa3230.exe"]

File System Events

Opens: C:\Windows\Prefetch\AE329AD95F7A6C49F8DACB3358AA3-94700DA4.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]