Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 196, Task ID: 784

Task ID:	784
Risk Level:	4
Date Processed:	2016-04-28 13:08:56 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\525a6ed3472d29161413f166baa05543.exe"
Sample ID:	196
Type:	basic
Owner:	admin
Label:	525a6ed3472d29161413f166baa05543
Date Added:	2016-04-28 12:45:10 (UTC)
File Type:	PE32:win32:gui
File Size:	35840 bytes
MD5:	525a6ed3472d29161413f166baa05543
SHA256:	8331e8b4881aca591f454faf4911e68716dde5b3dbec79f717545105627f4e88
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\525a6ed3472d29161413f166baa05543.exe
["C:\windows\temp\525a6ed3472d29161413f166baa05543.exe"]

File System Events

Opens: C:\Windows\Prefetch\525A6ED3472D29161413F166BAA05-7A6AC643.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\TaskHook.dll
Opens: C:\Windows\system32\TaskHook.dll
Opens: C:\Windows\system\TaskHook.dll
Opens: C:\Windows\TaskHook.dll
Opens: C:\Windows\System32\Wbem\TaskHook.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\TaskHook.dll

Windows Registry Events

Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]