Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 88, Task ID: 352

Task ID:	352
Risk Level:	5
Date Processed:	2016-04-28 12:56:46 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9003ab3119bca4c6bf6748d8cc07d9b7.exe"
Sample ID:	88
Type:	basic
Owner:	admin
Label:	9003ab3119bca4c6bf6748d8cc07d9b7
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	735648 bytes
MD5:	9003ab3119bca4c6bf6748d8cc07d9b7
SHA256:	2cb8860918a5d50377365116c6de297fcfed93dbdde0459afc5042f5f0786158
Description:	None

Pattern Matching Results

5 Possible injector
2 PE: Nonstandard section
4 Checks whether debugger is present

Static Events

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\windows\temp\9003ab3119bca4c6bf6748d8cc07d9b7.exe ["C:\windows\temp\9003ab3119bca4c6bf6748d8cc07d9b7.exe"]

File System Events

Opens: C:\Windows\Prefetch\9003AB3119BCA4C6BF6748D8CC07D-2CA75C14.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\9003ab3119bca4c6bf6748d8cc07d9b7.exe.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens: C:\windows\temp\LZ32.dll
Opens: C:\Windows\System32\lz32.dll
Opens: C:\windows\temp\WINSPOOL.DRV
Opens: C:\Windows\System32\winspool.drv
Opens: C:\Windows\System32\sechost.dll
Opens: C:\windows\temp\uz32_211.dll
Opens: C:\Windows\system32\uz32_211.dll
Opens: C:\Windows\system\uz32_211.dll
Opens: C:\Windows\uz32_211.dll
Opens: C:\Windows\System32\Wbem\uz32_211.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\uz32_211.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
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]