Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 198, Task ID: 793

Task ID:	793
Risk Level:	4
Date Processed:	2016-04-28 13:09:35 (UTC)
Processing Time:	2.79 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\52fd1e3fbd2bc9460fda9703084b404f.exe"
Sample ID:	198
Type:	basic
Owner:	admin
Label:	52fd1e3fbd2bc9460fda9703084b404f
Date Added:	2016-04-28 12:45:10 (UTC)
File Type:	PE32:win32:gui
File Size:	7680 bytes
MD5:	52fd1e3fbd2bc9460fda9703084b404f
SHA256:	155f5f74f8f362759ad305ff48055f199e23e64519bad1f5e39d50d791f7942f
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\52fd1e3fbd2bc9460fda9703084b404f.exe
["C:\windows\temp\52fd1e3fbd2bc9460fda9703084b404f.exe"]
Terminates process: C:\Windows\Temp\52fd1e3fbd2bc9460fda9703084b404f.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens: C:\Windows\Prefetch\52FD1E3FBD2BC9460FDA9703084B4-6F25EEB6.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\52fd1e3fbd2bc9460fda9703084b404f.exe.Local\
Opens:
C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742
Opens:
C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcr90.dll
Opens: C:\
Opens: C:\Windows\SysWOW64\wbem
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0
Opens: C:\Windows\Temp

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
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
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\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
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]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]