Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 241, Task ID: 964

Task ID:	964
Risk Level:	5
Date Processed:	2016-04-28 13:14:16 (UTC)
Processing Time:	2.76 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d02d9ed231437b31fcbb8b3f581987f5.exe"
Sample ID:	241
Type:	basic
Owner:	admin
Label:	d02d9ed231437b31fcbb8b3f581987f5
Date Added:	2016-04-28 12:45:15 (UTC)
File Type:	PE32:win32:gui
File Size:	196608 bytes
MD5:	d02d9ed231437b31fcbb8b3f581987f5
SHA256:	d829e38792f116d0636bb565cb0daaf0f3a0722f4ebb7859694ca76dc89af2da
Description:	None

Pattern Matching Results

5 Possible injector

Process/Thread Events

Creates process: C:\windows\temp\d02d9ed231437b31fcbb8b3f581987f5.exe
["C:\windows\temp\d02d9ed231437b31fcbb8b3f581987f5.exe"]
Terminates process: C:\Windows\Temp\d02d9ed231437b31fcbb8b3f581987f5.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens: C:\Windows\Prefetch\D02D9ED231437B31FCBB8B3F58198-57DCE9B7.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\sechost.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\System32\version.dll
Opens: C:\windows\temp\WINMM.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\Windows\System32\imm32.dll

Windows Registry Events

Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
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: 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

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\compsoft\doro
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
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]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[d02d9ed231437b31fcbb8b3f581987f5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]