

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 219, Task ID: 874

Task ID:	874
Risk Level:	4
Date Processed:	2016-04-28 13:11:41 (UTC)
Processing Time:	61.07 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\73c74c060890db0006f89fc31e55022a.exe"
Sample ID:	219
Type:	basic
Owner:	admin
Label:	73c74c060890db0006f89fc31e55022a
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	288784 bytes
MD5:	73c74c060890db0006f89fc31e55022a
SHA256:	0449b0d5d1fe843662306b8afadf24fd0391997a81e30129ede98f9b7b6b23bb
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\73c74c060890db0006f89fc31e55022a.exe
["C:\windows\temp\73c74c060890db0006f89fc31e55022a.exe"]	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
----------------	---

File System Events

Opens:	C:\Windows\Prefetch\73C74C060890DB0006F89FC31E550-60B15AC2.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\73c74c060890db0006f89fc31e55022a.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\appatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\winpool.drv

Windows Registry Events

Opens key:	HKLM\software\microsoft\wow64
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\system\currentcontrolset\control\ntp\customlocale
Opens key:	HKLM\system\currentcontrolset\control\ntp\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
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\appcompatflags\disable8and16bitmitigation
 Opens key: HKLM\system\currentcontrolset\control\session manager
 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: HKCU\software\microsoft\windows
 nt\currentversion\appcompatflags[showdebuginfo]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]