

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 88, Task ID: 350

Task ID:	350
Risk Level:	5
Date Processed:	2016-04-28 12:56:36 (UTC)
Processing Time:	63.14 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"]	

Named Object Events

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

File System Events

Opens:	C:\Windows\Prefetch\9003AB3119BCA4C6BF6748D8CC07D-2CA75C14.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\9003ab3119bca4c6bf6748d8cc07d9b7.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\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens:	C:\Windows\SysWOW64\lz32.dll
Opens:	C:\Windows\SysWOW64\usp10.dll
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\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
 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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 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]