

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 23, Task ID: 92

Task ID:	92
Risk Level:	4
Date Processed:	2016-04-28 12:48:54 (UTC)
Processing Time:	61.22 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\3d3153fe8f8692117697828274214ee6.exe"
Sample ID:	23
Type:	basic
Owner:	admin
Label:	3d3153fe8f8692117697828274214ee6
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	315392 bytes
MD5:	3d3153fe8f8692117697828274214ee6
SHA256:	06645c8156462a318598c1ec5ea070cfebde6031b9f696925e62f39ac36a91a6
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\3d3153fe8f8692117697828274214ee6.exe
	["C:\windows\temp\3d3153fe8f8692117697828274214ee6.exe"]

File System Events

Opens:	C:\Windows\Prefetch\3D3153FE8F8692117697828274214-E0A5C2B6.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\SysWOW64\sechost.dll
Opens:	C:\windows\temp\3d3153fe8f8692117697828274214ee6.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\WINSPOOL.DRV
Opens:	C:\Windows\SysWOW64\winpool.drv
Opens:	C:\windows\temp\oledlg.dll
Opens:	C:\Windows\SysWOW64\oledlg.dll
Opens:	C:\windows\temp\SLABHIDDevice.dll
Opens:	C:\Windows\SysWOW64\SLABHIDDevice.dll
Opens:	C:\Windows\system\SLABHIDDevice.dll
Opens:	C:\Windows\SLABHIDDevice.dll
Opens:	C:\Windows\SysWOW64\Wbem\SLABHIDDevice.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\SLABHIDDevice.dll

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\terminal server

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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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\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: 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]