Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3320, Task ID: 790

Task ID:	790
Risk Level:	6
Date Processed:	2016-05-18 10:38:38 (UTC)
Processing Time:	61.38 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\54b31207c61a234f126500151139a137.exe"
Sample ID:	3320
Type:	basic
Owner:	admin
Label:	54b31207c61a234f126500151139a137
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	580608 bytes
MD5:	54b31207c61a234f126500151139a137
SHA256:	1a29909df3d3dda23568f277f184ed8854674d75affeedb4ee5277bda9671b06
Description:	None

Pattern Matching Results

2 PE: Nonstandard section
6 Suspicious packer: VMProtect

Static Events

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\windows\temp\54b31207c61a234f126500151139a137.exe ["C:\windows\temp\54b31207c61a234f126500151139a137.exe"]

File System Events

Opens: C:\Windows\Prefetch\54B31207C61A234F126500151139A-E7AF4FDC.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\MFC42u.DLL
Opens: C:\Windows\SysWOW64\mfc42u.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\ODBC32.dll
Opens: C:\Windows\SysWOW64\odbc32.dll
Opens: C:\windows\temp\Mag_Hook.dll
Opens: C:\Windows\SysWOW64\Mag_Hook.dll
Opens: C:\Windows\system\Mag_Hook.dll
Opens: C:\Windows\Mag_Hook.dll
Opens: C:\Windows\SysWOW64\Wbem\Mag_Hook.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Mag_Hook.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\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
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]