

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3320, Task ID: 789

Task ID:	789
Risk Level:	6
Date Processed:	2016-05-18 10:38:35 (UTC)
Processing Time:	61.67 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:	1a29909df3d3dda23568f277f184ed8854674d75affedb4ee5277bda9671b06
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\System32
Opens:	C:\windows\temp\MFC42u.DLL
Opens:	C:\Windows\System32\mfc42u.dll
Opens:	C:\windows\temp\ODBC32.dll
Opens:	C:\Windows\System32\odbc32.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\Mag_Hook.dll
Opens:	C:\Windows\system32\Mag_Hook.dll
Opens:	C:\Windows\system\Mag_Hook.dll
Opens:	C:\Windows\Mag_Hook.dll
Opens:	C:\Windows\System32\Wbem\Mag_Hook.dll
Opens:	C:\Windows\System32\WindowsPowerShell\v1.0\Mag_Hook.dll

Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
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
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
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]