Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3334, Task ID: 845

Task ID:	845
Risk Level:	6
Date Processed:	2016-05-18 10:45:28 (UTC)
Processing Time:	62.28 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\758e49c5f3fae3fd55f5c26204023b81.exe"
Sample ID:	3334
Type:	basic
Owner:	admin
Label:	758e49c5f3fae3fd55f5c26204023b81
Date Added:	2016-05-18 10:30:52 (UTC)
File Type:	PE32:win32:gui
File Size:	344064 bytes
MD5:	758e49c5f3fae3fd55f5c26204023b81
SHA256:	0c71ca797853ba4553280fecadc2c082abd618e793e5bd718a8c6fd780abcc18
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\758e49c5f3fae3fd55f5c26204023b81.exe
["C:\windows\temp\758e49c5f3fae3fd55f5c26204023b81.exe"]

File System Events

Opens: C:\Windows\Prefetch\758E49C5F3FAE3FD55F5C26204023-D4C53B7A.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\sechost.dll
Opens: C:\windows\temp\758e49c5f3fae3fd55f5c26204023b81.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\mobsync.dll
Opens: C:\Windows\system32\mobsync.dll
Opens: C:\Windows\system\mobsync.dll
Opens: C:\Windows\mobsync.dll
Opens: C:\Windows\System32\Wbem\mobsync.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\mobsync.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
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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]