Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3306, Task ID: 733

Task ID:	733
Risk Level:	6
Date Processed:	2016-05-18 10:31:27 (UTC)
Processing Time:	61.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe"
Sample ID:	3306
Type:	basic
Owner:	admin
Label:	35644f3d0029f81c3d478d3c2407fac3
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	597504 bytes
MD5:	35644f3d0029f81c3d478d3c2407fac3
SHA256:	05093ba493e460b909f4922656c72a340517b31d8d6ff569dd73a2c1c9fc04dd
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\35644f3d0029f81c3d478d3c2407fac3.exe
["C:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe"]

File System Events

Opens: C:\Windows\Prefetch\35644F3D0029F81C3D478D3C2407F-83FCDD92.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\sechost.dll
Opens: C:\windows\temp\NETAPI32.dll
Opens: C:\Windows\System32\netapi32.dll
Opens: C:\windows\temp\netutils.dll
Opens: C:\Windows\System32\netutils.dll
Opens: C:\windows\temp\srvcli.dll
Opens: C:\Windows\System32\srvcli.dll
Opens: C:\windows\temp\wkscli.dll
Opens: C:\Windows\System32\wkscli.dll
Opens: C:\windows\temp\pdh.dll
Opens: C:\Windows\System32\pdh.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]