Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 17, Task ID: 67

Task ID:	67
Risk Level:	1
Date Processed:	2016-04-28 12:48:26 (UTC)
Processing Time:	63.3 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7a40d76e9fa341618d44f168752f6c0f.exe"
Sample ID:	17
Type:	basic
Owner:	admin
Label:	7a40d76e9fa341618d44f168752f6c0f
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	61440 bytes
MD5:	7a40d76e9fa341618d44f168752f6c0f
SHA256:	4d27b0fd517894fd083418585b34b5497c14dfdbf006241a525d954700804a92
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\7a40d76e9fa341618d44f168752f6c0f.exe ["C:\windows\temp\7a40d76e9fa341618d44f168752f6c0f.exe"]

File System Events

Opens: C:\Windows\Prefetch\7A40D76E9FA341618D44F168752F6-E5A6DC7D.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\MFC71.DLL
Opens: C:\Windows\system32\MFC71.DLL
Opens: C:\Windows\system\MFC71.DLL
Opens: C:\Windows\MFC71.DLL
Opens: C:\Windows\System32\Wbem\MFC71.DLL
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\MFC71.DLL

Windows Registry Events

Opens key: HKLM\system\currentcontrolset\control\session manager
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\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\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: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]