Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 83, Task ID: 333

Task ID:	333
Risk Level:	6
Date Processed:	2016-04-28 12:56:09 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\904a88847df33f9dc01514e65f74a382.exe"
Sample ID:	83
Type:	basic
Owner:	admin
Label:	904a88847df33f9dc01514e65f74a382
Date Added:	2016-04-28 12:44:58 (UTC)
File Type:	PE32:win32:gui
File Size:	805376 bytes
MD5:	904a88847df33f9dc01514e65f74a382
SHA256:	65dc196f7e1e23f6ee8cb6edc0f6e7b0db51d2c9c36d1463207ecb00eebdc400
Description:	None

Pattern Matching Results

6 PE: File has TLS callbacks
2 PE: Nonstandard section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: File contain TLS callbacks

Process/Thread Events

Creates process: C:\windows\temp\904a88847df33f9dc01514e65f74a382.exe
["C:\windows\temp\904a88847df33f9dc01514e65f74a382.exe"]

File System Events

Opens:	C:\Windows\Prefetch\904A88847DF33F9DC01514E65F74A-10326009.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\libdolphinprivate.dll
Opens:	C:\Windows\SysWOW64\libdolphinprivate.dll
Opens:	C:\Windows\system\libdolphinprivate.dll
Opens:	C:\Windows\libdolphinprivate.dll
Opens:	C:\Windows\SysWOW64\Wbem\libdolphinprivate.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\libdolphinprivate.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\terminal server

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
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\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]