Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 201, Task ID: 804

Task ID:	804
Risk Level:	6
Date Processed:	2016-04-28 13:09:42 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\c0d7007dfdc093732bcae8144bab71d5.exe"

Sample ID:	201
Type:	basic
Owner:	admin
Label:	c0d7007dfdc093732bcae8144bab71d5
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	79360 bytes
MD5:	c0d7007dfdc093732bcae8144bab71d5
SHA256:	3f42f77aa67f34c41b46d17de28ca58f7ff3061e198f1cba2fcd08e351f67b92
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\c0d7007dfdc093732bcae8144bab71d5.exe ["C:\windows\temp\c0d7007dfdc093732bcae8144bab71d5.exe"]

File System Events

Opens:	C:\Windows\Prefetch\C0D7007DFDC093732BCAE8144BAB7-BF62272C.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\Qt5Core.dll
Opens:	C:\Windows\system32\Qt5Core.dll
Opens:	C:\Windows\system\Qt5Core.dll
Opens:	C:\Windows\Qt5Core.dll
Opens:	C:\Windows\System32\Wbem\Qt5Core.dll
Opens:	C:\Windows\System32\WindowsPowerShell\v1.0\Qt5Core.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
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]