Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 136, Task ID: 544

Task ID:	544
Risk Level:	6
Date Processed:	2016-04-28 13:01:57 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9bc18ad1dd5ea3d0b81ced065eae9e3d.exe"
Sample ID:	136
Type:	basic
Owner:	admin
Label:	9bc18ad1dd5ea3d0b81ced065eae9e3d
Date Added:	2016-04-28 12:45:04 (UTC)
File Type:	PE32:win32:gui
File Size:	620032 bytes
MD5:	9bc18ad1dd5ea3d0b81ced065eae9e3d
SHA256:	361488dd460f77d179f6f29664f9431645998fa947fa1f7fbfa3cedb0e8d3fed
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\9bc18ad1dd5ea3d0b81ced065eae9e3d.exe ["C:\windows\temp\9bc18ad1dd5ea3d0b81ced065eae9e3d.exe"]

File System Events

Opens:	C:\Windows\Prefetch\9BC18AD1DD5EA3D0B81CED065EAE9-CCEF0519.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\libkcmutils.dll
Opens:	C:\Windows\system32\libkcmutils.dll
Opens:	C:\Windows\system\libkcmutils.dll
Opens:	C:\Windows\libkcmutils.dll
Opens:	C:\Windows\System32\Wbem\libkcmutils.dll
Opens:	C:\Windows\System32\WindowsPowerShell\v1.0\libkcmutils.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]