Anubis - Analysis Report

Analysis Report for 71cbffccc64b8cfc386f963435ca3cbc

MD5: 71cbffccc64b8cfc386f963435ca3cbc

Summary:

No threats could be detected by Anubis. This does **not** imply that execution of this executable is safe.

International Secure Systems Lab
Vienna University of Technology , Eurecom France , UC Santa Barbara
Contact: anubis@iseclab.org

Dependency overview:

71cbffccc6.exe C:\71cbffccc6.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information..... 4
2. 71cbffccc6.exe..... 4
   a) Registry Activities..... 4
   b) File Activities..... 4

1. General Information

Information about Anubis' invocation	
Time needed:	254 s
Report created:	03/19/11, 11:12:37 UTC
Termination reason:	Timeout
Program version:	1.75.3394

2. 71cbffccc6.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	71cbffccc6.exe
MD5:	71cbffccc64b8cfc386f963435ca3cbc
SHA-1:	bd3f180310f163cd74ecad6e7f050f5039522759
File Size:	91151
Command Line:	"C:\71cbffccc6.exe"
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\user32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\WinSxS\ x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\ gdiplus.dll	0x4EC50000	0x001A6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000

2.a) 71cbffccc6.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1

2.b) 71cbffccc6.exe - File Activities

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1

Memory Mapped Files:

File Name
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\gdiplus.dll