Anubis - Analysis Report

Analysis Report for 54026447

MD5: 33f6e4adda37abcea34c02adc2ebadd7

Summary:

Description	Risk
AV Hit: This executable is detected by an antivirus software.	high

Dependency overview:

54026447.exe C:\54026447.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information..... 4
2. 54026447.exe.....4
   a) Registry Activities.....4
   b) File Activities..... 4

1. General Information

Information about Anubis' invocation	
Time needed:	259 s
Report created:	09/14/11, 01:06:42 UTC
Termination reason:	Timeout
Program version:	1.75.3394

2. 54026447.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	54026447.exe
MD5:	33f6e4adda37abcea34c02adc2ebadd7
SHA-1:	4b079a22d99cb6f8d827c78bcd038856c7512b41
File Size:	284160
Command Line:	"C:\54026447.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\system32\advapi32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\oleaut32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\winmm.dll	0x76B40000	0x0002D000

Ikarus Virus Scanner

Virus.Win32.Dracur (Sig-Id:1427994)

2.a) 54026447.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\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1

2.b) 54026447.exe - File Activities

Files Read:

C:\54026447.exe

PIPE\InitShutdown

PIPE\winreg

Files Modified:

PIPE\InitShutdown
PIPE\winreg

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1
PIPE\InitShutdown	0x0011C017	1
PIPE\winreg	0x0011C017	1

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8

Memory Mapped Files:

File Name
C:\WINDOWS\system32\winmm.dll