Anubis - Analysis Report

Analysis Report for d9c2c1f74e5d260bddc21bd6cd599161.amada

MD5: d9c2c1f74e5d260bddc21bd6cd599161

Summary:

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

Dependency overview:

d9c2c1f74e.exe C:\d9c2c1f74e.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information..... 4
2. d9c2c1f74e.exe..... 4
   a) Registry Activities..... 4
   b) File Activities..... 4

1. General Information

Information about Anubis' invocation	
Time needed:	241 s
Report created:	02/23/11, 18:39:31 UTC
Termination reason:	Timeout
Program version:	1.74.3362

2. d9c2c1f74e.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	d9c2c1f74e.exe
MD5:	d9c2c1f74e5d260bddc21bd6cd599161
SHA-1:	0276be96bbe638be977775c3ca55d1ebc84af471
File Size:	176128
Command Line:	"C:\d9c2c1f74e.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\MSVBVM60.DLL	0x73420000	0x00153000
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\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000

Ikarus Virus Scanner

Trojan.Win32.Menti (Sig-Id:52193694)

2.a) d9c2c1f74e.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
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
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Language Hotkey	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Layout Hotkey	2	2

2.b) d9c2c1f74e.exe - File Activities

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8

Memory Mapped Files:

File Name
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\MSVBVM60.DLL
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\rpcss.dll