



Anubis - Analysis Report



Analysis Report for e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f95599 MD5: f7a0f8d044c333ad3b7d65a6485af931

Summary:

Description	Risk
Performs Registry Activities: The executable reads and modifies register values. It also creates and monitors register keys.	● low

Dependency overview:



a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991 C:

\a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information.....	4
2. a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991.....	4
a) Registry Activities.....	4
b) File Activities.....	4



1. General Information

Information about Anubis' invocation

Time needed:	240 s
Report created:	09/24/09, 21:50:04 UTC
Termination reason:	Timeout
Program version:	1.72.0

2. a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991

General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991
MD5:	f7a0f8d044c333ad3b7d65a6485af931
SHA-1:	a381aed69ed753618e0b3930c78243701af44d7d
File Size:	29184
Command Line:	"C:\a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991"
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

2.a) a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991 - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Control\Terminal Server	TSEAppCompat	0	2

2.b) a2e722bad96734a23eff0c447d280831-742957ec4ac245538985d6e8f9559991 - File Activities

File System Control Communication:

File	Control Code	Times
C:\	0x00090028	1