Subject: Re: Tracer
Posted by gridem on Tue, 09 Jun 2009 14:33:21 GMT
View Forum Message <> Reply to Message

Some comments how to start the program.

1. Execute 'trace.exe':

E:\Tracer>trace.exe
Please, find 'input.xml' file and edit it

2. Edit file 'input.xml', e.g.:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE input>
<input>
 <hooks>
  <item>CloseHandle</item>
  <item>CreateThread</item>
  <item>LoadLibraryExW</item>
 </hooks>
 <exepath>c:\windows\notepad.exe</exepath>
 <exeargs></exeargs>
</input>
```

3. Execute 'trace.exe' again, see the result like:

```
E:\Tracer>trace.exe
Begin
Listen was started
Process is created
DLL was injected
Detached cave memory
Resumed process
Waiting for program ending...
Pipe was connected
The pipe has been ended.
Listen completed successfully
Program was finished successfully
```