Subject: Tracer

Posted by gridem on Tue, 09 Jun 2009 08:26:23 GMT

View Forum Message <> Reply to Message

I am glad to introduce the program 'tracer'.

The application catches the started program calls to kernel32.dll on Windows 32 bit platform. This application tested on the following platforms: Windows XP 32 bit, Windows 2003 Server 2003 x64, Windows Vista x32, Windows 7 Beta x32. Now it works for only 32 bit programs.

The program was written using, of course, U++ and some private engines. I think that this program will be useful for developers on Windows platforms.

Download link

Subject: Re: Tracer

Posted by Novo on Tue, 09 Jun 2009 11:53:51 GMT

View Forum Message <> Reply to Message

```
c:\local\work\download\1>trace dir.exe
Begin
Listen was started
EERRRORR: OTR in listen: Nheo sy sprocesstem cannot find t hei sfile speci fied.
o
n the other end of the pipe.
```

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
```