# Problem of existence of unlimited access to powerful tools of debugging in Windows

## 1. Problem description

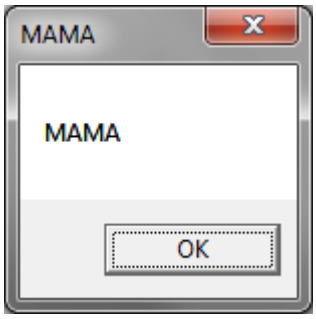
Existence in open access of powerful mechanisms of debugging of Windows allow the malefactor to make changes to the software secretly. The specified mechanisms can be used for creation of powerful tools of illegal control of the software in interests of the malefactor.

## 2. Problem demonstration

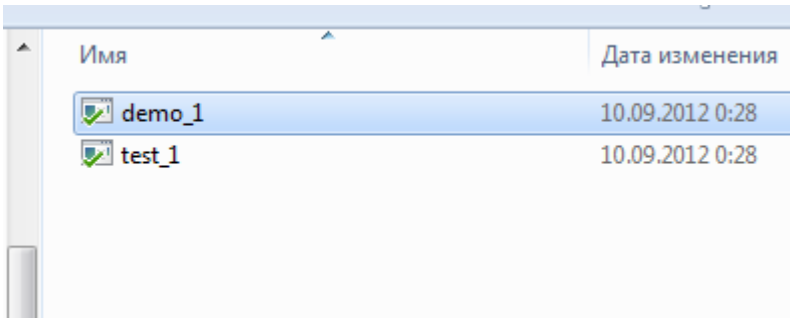
### a. Substitution of a data of the program

In the DEMO\demo_1\ folder two files are located: demo_1.exe and test_1.exe.

If we start on performance the demo_1.exe program that we will receive on the computer screen the following simple MessageBox window:

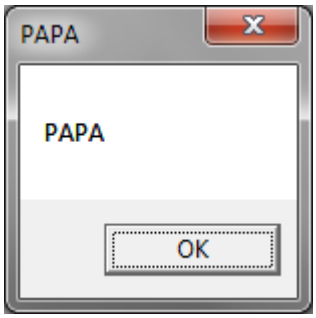



Let's start the test_1.exe program and we will choose for start the demo_1.exe program:




The test_1.exe program starts the demo_1.exe program in a mode of debugging and uses debugging functions and as the ReadProcessMemory and WriteProcessMemory functions.

Thus, the test_1.exe program substitutes in memory of the demo_1.exe program. As a result of demo_1.exe program work we will see already other result:

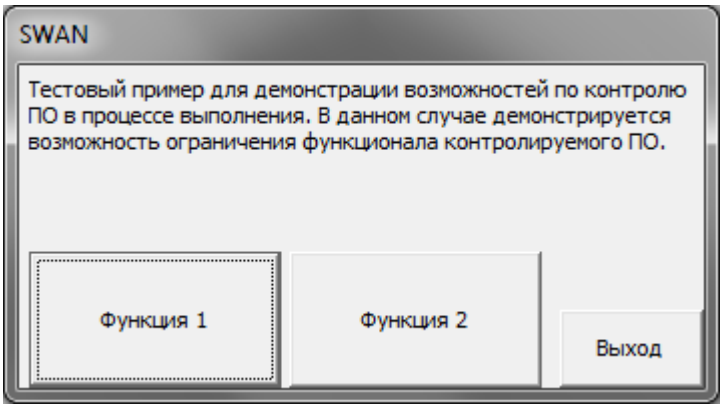



Thus, the malefactor has opportunity secretly for the user to change data in the software.

**b. Substitution of a code of the program**

In the DEMO\demo_2\ folder two files are located: demo_2.exe and test_2.exe.

If we start on performance the demo_2.exe program that we will receive on the computer screen the following simple window:




In the demo_2.exe program all buttons function.

Let's start the test_2.exe program and we will choose for start the demo_2.exe program.

The test_2.exe program starts the demo_2.exe program in a mode of debugging and uses debugging functions and as the ReadProcessMemory and WriteProcessMemory functions.

Thus, the test_2.exe program substitutes in memory of the demo_2.exe program. As a result of demo_2.exe program work we will see already other result: in the demo_2.exe program the average button doesn't function.

The test_2.exe program secretly changes algorithm of functioning of the demo_2.exe program started in a mode of debugging.

## 3. Offers on a solution

### a. Simple level

It is necessary to realize the prevention of the user of Windows of use of debugging mechanisms.

### b. Average level

To enter into use along with a role "Administrator" a role "Developer".

This role has to be disconnected by default and join is in addition public.

To limit use of powerful mechanisms of debugging and other powerful functions connected with development of the software only in a context of a role of "Developer".

### c. Powerful level

This level can include methods of the previous level and in addition:

To forbid use of debugging facilities for the signed programs.

To realize a paradigm "Developer". Only the signed developer has access to mechanisms of debugging and development of the software in a context "Developer". Only the signed developer can debug programs him signed.

To exclude from standard delivery of Windows of a debugging facility. Inclusion of debugging facilities can happen in addition.

Evgenie Rodygin

e.v.rodigin@live.ru