**Hardware Breakpoints​ dots stop ).** Wonderful thing and at this and also

deficit - total four on every process . Points checked 2 times ( all four ). Process

installations their own hardware dots looks like next way :

1. Management receives instruction **UD2** , on which Always is happening exception (Illegal

(instructions)

2. SEH- handler for UD2 looks like next way :

PUSH EBP

MOV EBP,ESP

PUSHAD

MOV EAX,DWORD PTR SS:[EBP+8]

MOV EAX,DWORD PTR DS:[EAX]

MOV EAX,DWORD PTR DS:[12129F0]

MOV DWORD PTR DS:[ 12022A0],EAX

MOV DWORD PTR DS:[ 12022A4],26182AEF <- MOV DWORD PTR DS:[12022A4],26182AED (2nd)

MOV DWORD PTR DS:[ 12022A8],EBP

PUSH OFFSET 012022A0

CALL 00D44F40

MOV DWORD PTR DS:[ 12022A0],0

MOV DWORD PTR DS:[ 12022A4],0

MOV DWORD PTR DS:[ 12022A8],0

POPAD

XOR EAX,EAX

MOV ESP,EBP

POP EBP

RETN

Their at all two : **00C996B0h** and **00C99702h** – for first 4 HB and accordingly For second .

3. Before Togo How go to Securomov's SEH handler , control Always beret on myself

ntdll.KiUserExceptionDispatcher ( pExeptionRecord , pContext ). Second argument - link

on structure context . CALL 00D44F40 leads to the VM, which changes in the stack structure

Context **(** DR0, DR1, DR2, DR3 **).**

4. *Focus ! Focus !* After exit from handler is being carried out **ZwContinue** on next from UD2

instructions **,** with already Securomovsky context , i.e. with its hardware dots stop .

5. Hardware (DR0-DR3) is triggered dot installation .

6. SEH- handler ( VM) checks context , address (in which happened exceptions ) and more

will fit into DR7 control meaning . If What Not so - to you will give know ! :)

**Software dots stop and overlap code .** If hardware points stop was given

intent attention , but What speak for software . First of all queue All starts with

mentioned higher trick :

MOV EAX,11D7B1C

MOV ESI,DWORD PTR DS:[EAX]

ADD DWORD PTR SS:[ ESP+10],ESI …

To repeatedly complicate tracing and detection important asm instructions and procedures

under consideration code , you can say , overlaps distance between them . Because of what sit and

press F7, F8 or include animated tracing so same useless as peas​​ up

wall ". Developers they expected that the reversers will be handed over nerves , and they will be to procreate

software dots stop , how rabbits - to faster go out from this traps . As a result

control sum plot is violated and instead desired places appointments , protector sends

unlucky hackers there the same as Makar​ calves Not drove . If such big wish

trace , then fight it​ you can . First of all , the trap characteristic his own

cycle, PUSHFD /POPFD and the following conditional transition . Therefore figure out where will transmitted

control , bypassing at this cycle , it's not difficult . Secondly , hardware dots stop are checked in

sum only 8 times ( 2 by 4) in the very at the beginning , so What equipment for us .

By the way, in ≪ Safe disk ≫ *aka* SafeDisk in the role overlapping code serve ≪ frogs ≫ -

scattered conditional and unconditional conditional transitions working​ By to the same one same paths .

Undoubtedly conditional transitions , this is when ( the most common option ):

XOR EAX, EAX

JZ SOME\_LABEL

Despite on That What opcode transition Not **JMP** , jump He on SOME\_LABEL will be **always !** Happens

This because​​ result operations ≪ *exclusive OR* ≫ on one and the same same register Always -

**ZERO!( NULL, ZERO, 0, donut ).** Accordingly flag **Z** ( Zero Flag) processor will cocked

( is equal to unit ) and yours processor , obeying cocked **Zero Flag** , will execute condition transition .

**Examination software**

**Examination software dots stops / transitions at the beginning WinAPI .** Install software dots

stop at start / end procedures at all is standard de facto that here speak . Good

are being checked Not All WinAPI , but in the list got there *CreateFileA* , *FindWindow* . Opposition .

The most the obvious is not put software dots stop on first instructions . Optional

even on​ the second one . For example , like standard *CreateFileA* generates a UNICODE string and calls

*CreateFileW* , then Can put it on and call *CreateFileW* . Other the matter with adapters . How

no spin , but put their comfortable at first , because in most cases hooked WinAPI first three

instructions ( prologue ):

MOV EDI, EDI

PUSH EBP

MOV EBP, ESP

For counteracting X- code will be required table export systemic libraries and table

import images and that the fact is that compiler For alignments functions By multiple addresses

leaves place between them . In the first case , raw bias need to move up on one

byte , and at this we get into ( any case should get ) to NOP, and in second case We already

Let's fix the RVA functions . Thus thus , minimally alterations we'll force tread check

NOP, and transition below will remain safe . Kol speech went about the table export , no superfluous

will mention that​ on *GetProcAddress* Sometimes Also healthy put mine handler ! \_ \_