**DeviceIoControl ( 4 TIMES )** . Main role Here took away DeviceIoControl , with whose with help Can All

What whatever you like do or get from device . Before total important ControlCode , which Maybe

accept three meanings :

1) ( *IOCTL\_SCSI\_PASS\_THROUGHT\_DIRECT* ) **4D014** h or **4D004** h. Priority opportunity is

information about the physical availability disk in the device . Then is coming various information about

tracks , sectors , etc. Size​ buffers Always equals 50h(80 bytes).

**CMP BYTE PTR SS:[ EBP-52],BL // Inserted li disc in tray ?**

First examination only For confirmations availability disk in the drive . If everything is OK then let's start

procedure reading and composing signatures .

On this stage , at execution *WinAPI* **DeviceIoControl ,** please contact attention on

**InBuffer ( ESP+8): from beginning InBuffer By offset $+14h** is located pointer on structure special .

buffers , where , after execution call , lie down service data ( *eg number​ sectors* ).

Correct passage first from checks ( and subsequent ones ), forces **SecuROM** 7-8 generate

repeat message : *Cannot authenticate the original disc* . *Your disc may require a different software version.*

True , there is more 4 check , but her patching Not influences finite on result - *Level 1 completed!*

**IMPORTANT! Patch need to directly operations that affect on flags , not ourselves transitions ! PUSHFD protection saves state**

***EFL* for following transitions (in 7.33.017 their Not more than 2x), i.e. the condition is being checked some once .**

**010B6FCE 83E0 1F AND EAX,0000001F**

**010B6FD1 3C 1F CMP AL,1F** // **AL** should be equal ***0x1 F( 31)*** or multiple to this number

**010B6FD3 9C PUSHFD**

**………………………………**

**010B7036 9D POPFD**

**010B7037 90 NOP**

**010B7038 75 17 JNE SHORT 010B7051 // TRANSITION NOT EXECUTED**

**\*\*\* 2 \*\*\***

**010A615 E . 8498 C0070000 TEST BYTE PTR DS:[ EAX+7C0],BL //BL = 1. it is clear that structure . [EAX+7C0] = 9 ( worked with any ! = 1)**

**………………………………**

**010B7038 75 17 JNE SHORT 010B7051 //TRANSITION NOT EXECUTED**

**\*\*\* 3 \*\*\***

**010B86A1 80BF F2070000 CMP BYTE PTR DS:[ EDI+7F2],0 //[EDI+7F2] = 1 ( also rolled with others numbers )**

**010B86A8 9C PUSHFD**

**………………………………**

**010B86AE 75 17 JNE SHORT 010B86C7 //TRANSITION IN PROGRESS**

**THE LAST TWO CHECKS (AT LEAST 2) ARE DIRECTLY RELATED TO LEVEL 2 AND MOST LIKELY SET THE LIMITS OF THE HIT INTERVAL**

*VIRTUAL BACKUP - REAL PHYSICAL* **( or CYCLE, NUMBER OF ITERATIONS).**

**By the way** , it's typical detail in this versions For first signature checks – ≪ fake ≫

count control amounts plot in the overlapping code .

**QueryPerformanceCounter** & **QueryPerfomanceFrequency** . Start count beats in normal

( preparatory mode ).

**LEVEL 2 \*\*\*\*\*\*\* CHECK GEOMETRY(CIRCUIT)** OR **QPC/QPF \*\*\*\*\*\*\***

**SetSystemCursor .** Temp.ani

*Here All more difficult and moment writing these lines , very depended from luck ( All*

*the problem is in the counting bug interval ).* ***The most The main thing*** *– it worked (* ***AND MORE THAN ONCE!!!):***

*launch with* ***absolutely left disk*** *in virtual drive ( Windows 7 installer ). ;)*

After of how​ on the 7th with linden virtual disk All passed ok , decided try on

8m without *Daemon Tools* with regular physical drive and disk . After successful passage

signature level process Always became terminate with code exit 1. First thought that​ This

protection . But Then remembered for ***HKEY\_CURRENT\_USER\Software\ SecuROM .*** Deleted branch **Key** – process

became to end Now **after** passage geometric checks (in **Bin** tables , structures

data checks By time and geometry , label disk under *XOR* and something more ) ***.***

In short ≪ fiscal ≫( *010 DF7A9* ) as shown on picture below ( *signed int* > 0). If Very

Interesting dig check - we put breakpoint By access .

**All What connected with second level - related to FPU operations .**

If Not will passed one from checks - process will end or will fall out exception .

Between checks and after the 3rd one is performed login to VM on specially designated islets .

***First adjustable examination second geometric level***

**010EAFB2 FLD QWORD PTR DS:[ 11EDC78]**

**010EAFB8 MOV ESI,OFFSET 012D1E30**

**010EAFBD FSUB QWORD PTR DS:[ 11EDC80]**

**010EAFC3 FMUL QWORD PTR DS:[ 14AC050]**

**010EAFC9 FCOMP QWORD PTR DS:[ 1483098]**

**010EAFCFFSTSWAX //AH == 0**

**010EAFD1 TEST AH,05**

**010EAFD4 PUSHFD**

**010EAFD5 PUSH 17F7**

**010EAFDA JPE SHORT 010EAFF 0 ; NOT TAKEN**

***Second adjustable examination second geometric level***

**010ED310 FLD QWORD PTR DS:[ 11EDC78]**

**010ED316 FSUB QWORD PTR DS:[ 11EDC80]**

**010ED31C FMUL QWORD PTR DS:[ 14A4E64]**

**010ED322 FCOMP QWORD PTR DS:[ 1483098]**

**010ED328FSTSWAX**

**010ED32A TEST AH,05 //AH == 1**

**010ED32D PUSHFD**

**010ED32E PUSH 24F2**

**010ED333 JPO SHORT 010ED34 A ; TAKEN!**

***The third adjustable duplicated examination second geometric level***

***010CD164 FLD QWORD PTR DS:[ 11EDC78]***

***010CD16A FSUB QWORD PTR DS:[ 11EDC80]***

***010CD170 FMUL QWORD PTR DS:[ 14A4E64]***

***010CD176 FCOMP QWORD PTR DS:[ 1483098]***

***010CD17CFSTSWAX***

***010CD17E TEST AH,05***

***010CD181 PUSHFD***

***010CD182 PUSH 14D***

***010CD187 MOV ESI,ESI***

***010CD189 JPE SHORT 010CD1A0***

***Correction mistakes “Conflict with Emulation Software detected” :***

***at request DeviceIoControl with macro IOCTL\_DISK\_PERFORMANCE (0x00070020) from minor***

***streams ( parallel examination geometry ), it is necessary return 0 ( zero ) in EAX. Sometimes helps***

***setting ( SetAffinityMask ) the minimum quantity permitted processors ( total one ) for***

***work of the target process .***

***Exists Also special function that​ requests codes exit streams :***

***010F146C PUSH EBP***

***010F146D MOV EBP,ESP***

***010F146F PUSH EBX***

***010F1470 PUSH ESI***

***010F1471 MOV ESI,DWORD PTR SS:[ARG.1]***

***010F1474 XOR EBX,EBX***

***010F1476 CMP BYTE PTR DS:[ ESI],BL***

***010F1478 PUSH EDI***

***010F1479 JE SHORT 010F14C7***

***010F147B CMP BYTE PTR DS:[ ESI+1],BL***

***010F147E JE SHORT 010F14C7***

***010F1480 PUSH EBX ; /Timeout => 0***

***010F1481 PUSH 1 ; | WaitAll = TRUE***

***010F1483 LEA EDI,[ ESI+228] ; |***

***010F1489 PUSH EDI; | HandleList***

***010F148A PUSH DWORD PTR DS:[ ESI+4] ; |Count***

***010F148D MOV DWORD PTR SS:[ ARG.1],EBX ; |***

***010F1490 CALL DWORD PTR DS:[ <&KERNEL32.WaitForMul ; \KERNEL32.WaitForMultipleObjects***

***010F1496 TEST EAX,EAX***

***010F1498 JE SHORT 010F149E***

***010F149A PUSH 5***

***010F149C JMP SHORT 010F14C9***

***010F149E CMP DWORD PTR DS:[ ESI+4],EBX***

***010F14A1 JLE SHORT 010F14BE***

***010F14A3 LEA EAX,[ ARG.1]***

***010F14A6 PUSH EAX ; / pExitCode => OFFSET ARG.1***

***010F14A7 PUSH DWORD PTR DS:[ EDI] ; | hThread***

***010F14A9 CALL DWORD PTR DS:[ <&KERNEL32.GetExitCo ; \KERNEL32.GetExitCodeThread***

***010F14AF CMP DWORD PTR SS:[ ARG.1],1***

***010F14B3 JNE SHORT 010F14C3***

***010F14B5 INC EBX***

***010F14B6 ADD EDI,4***

***010F14B9 CMP EBX,DWORD PTR DS:[ESI+4]***

***010F14BC JL SHORT 010F14A3***

***010F14BE XOR EAX,EAX***

***010F14C0 INC EAX***

***010F14C1 JMP SHORT 010F14CA***

***010F14C3 PUSH 6***

***010F14C5 JMP SHORT 010F14C9***

***010F14C7 PUSH 7***

***010F14C9 POP EAX***

***010F14CA POP EDI***

***010F14CB POP ESI***

***010F14CC POP EBX***

***010F14CD POP EBP***

***010F14CE RETN***

***Relatively files embedded in the protector and created in temporal folder . I wanted to would***

***remind that​ access in temporary folder Maybe be closed , so functions located in​***

***drm\_dyndata\_7330017.dll, can be duplicated in the image .***

***Well , now it's virtual. car ! Let's meet !***

***· Paul.dll ( pasha.dll )***

***Paul is possible Not patch . Enough fake results . Previously in Secura were constants answer paul . In the style of 21- no***

***passed check 1- passed . Or on the contrary . More was something type list addresses funk security in memory ( type IAT). So here in***

***this IAT secura were addresses type " check Not passed " and " passed examination online activations ". Stupidly changing 3 dword***

***in places Can was Always go By necessary branch . How now - I don't know .***

***Nightshade***

***VIRTUAL MATHEMATICS*** \_\_