SecuROM

« *If we associate SecuROM v7.33.17 with an Abrams tank without dynamic protection, OllyDbg with an RPG-7 grenade launcher, and X-code injection with a cumulative grenade for a grenade launcher, then, as in reality, such a backward shot will pierce the armor of this heavy and unwieldy machine and reach its target - OEP. The disabled machine is being studied by Russian engineers...* »

- Tiberium Reversal

SecuROM™† **SecuROM** (*secur, secure, sekira*) — protection against copying by evil pirates and idle hackers of these

games of yours and all other bullshit®, protected by copyright™ and distributed on electronic media. Unlike the shitty StarForce ™, it is loved by hackers and therefore is known for its low hack resistance: by default, the cracked version appears on torrents in a maximum of two days, in the worst case — in a couple of hours. By analogy with the last two versions of Windows , the **7.3x** line is most revered by crackers , while the latest, **8** , version is a copy of 7.35 slightly less than completely. On planet Earth, this creation was released by the bourgeois company Sony DADC AG, which, in addition to stamping CD/DVD blanks, decided to make money primarily from famous studios aka greedy developers,

and what's most interesting is that it did make money, but with groaning and scandals . In the end, in 2013, it was successfully buried by our hackers from *cracklab* ... so that in 2014, like a chrysalid hatched from a zombie , it would appear in the form of a fork of version 7 of the subject - *DENUVO* .

Content

They disassembled, took it apart and danced on the coffin lid.

Birth

Back in 1999, when the boorish drug companies for gamers started to slowly freak out from the spread of piracy in this country and the surrounding areas , SUDDENLY, out of nowhere, a certain Austrian Jew Reinhard Blaukovich showed up . Under the pretext of kicking the ass of unbridled hackers, he suggested Sony DADC create a new protection for gaming companies and publishers . The idea was received with enthusiasm by Sony, so Blaukovich quickly put together a team of developers , came up with a name for the protection system and began to slowly promote the subject to the masses.

Blaukovich is sad - he read "Tiberium Reversal" to the end. Canonical photo

"With love, Electronic Arts and Take 2 Interactive"

The developers are already discussing the next version

Sign: Reigard tries himself in big-time sports - SecuROM developers will soon be thrown out into the cold

LEGO Reinhardt™ looks at you like you're a victim of copyright.

| More athletic Reinhard Blaukovich	[expand]

Reasons for love

« *British scientists have proven that if your game is protected by SecuROM, crackers' interest in it increases by an average of 101 to 200%*

»

— **British Anonymous**

Quite banal:

Well, what else can one say here...

- By reversing SecuROM, you can learn and adopt a lot without ever vomiting from shitty coding .
  The thing is that, unlike some of the domestic star-crazed people, the developers of the subject do not suffer from paralysis of the upper limbs, arbid dysfunction of the brain, annihilation of the optic nerves, off-scale self-esteem and other manifestations of clumsiness.
- Each version has something new .
- Jokes inside.
- Whole jokes in later versions.
- User friendly interface from **drm_dialogs.dll**
- The subject is usually defended by the most widely known projects (GTA , Command & Conquer, BioShock, Witcher, WarCraft III, FarCry 2).
- The effect of the first hack is sure to bring incredible ecstasy to all participants (crackers, developers, publisher, ordinary users), and the hacker's %nickname is sure to be noted by the Internet community and even in the news.
- ???????
- MOV EAX, DEADC0DE
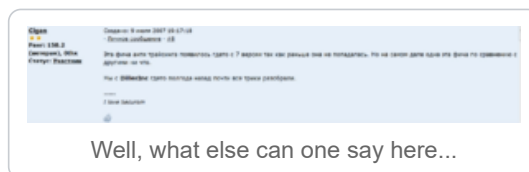
Explanation in one quote	[expand]

SecuROM in Russia

In this country, little is known about SecuROM and Sony Dadz in general, so there is only one myth that SecuROM is supposedly a shitty protection and breaks down faster than AvtoVAZ products . In fact, this myth is actively promoted in magazine articles, the authors of which were bought out by Protection Technology and now sing the praises of the

domestic manufacturer on every piss-stained corner (http://www.lki.r u/text.php?id=4868) . The fact is that all the well-known large studios (Electronic Arts, Take-Two Interactive) that stamp out games are located in the West. The latter, having developed legislation and common sense, simply sent this stellar crap to hell and told its authors to go to hell, thereby giving the opportunity to vacuum up money from game publishers only to Sony DADC, accomplices from Macrovision Corporation, and a little bit to the frogs with their dull solido shield. In general, the dream of hundreds of oil and worldwide recognition for the guys from Protection Technology has collapsed.

However, the peak of der-Emization was in 2005-2009 (2007±2), and after a long series of fails, Reinhard began to understand that the hour was not far off when SecuROM would be equipped with a wooden Macintosh, and funeral music would start playing in Sony DADC AG, but the subject would not hear it. In order to somehow save the situation, a friendship was made with some branch of ZOG called Tribeka. However, statistics inexorably show that the subject is no longer a cake and is slowly sliding from the winrar Warcraft III, GTA, CnC, FarCry, MassEffect to defending pop crap from Walt Disney studios like Brave Video Game (http://www.ag.ru/games/brave-the-video-game) or Disney Princess: My FairyTale Adventure (http://www.ag.ru/games/disney-princess-my-fairytale-adventure) , which is intended for younger children . But strangely enough, modern youth don't give a damn about such games - don't feed them bread, let them shoot in Battlefield 3 or Counter-Strike. Therefore, sales of children's Disney crafts are supported by bad hackers of Slavic nationality, who buy this only because~~play~~disassemble the guts of the new version of Securo and get another portion of lulz. That's bullshit, kids !
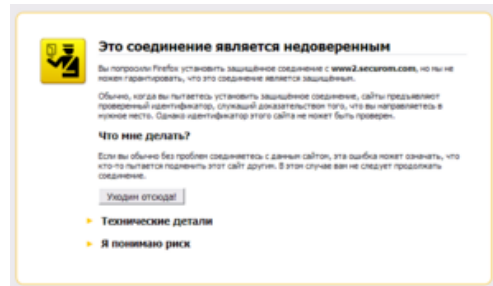
Fire Fox does not recommend hanging around the websites of DRM manufacturers!

SolidShield[expand]

Scandals and Fails

Locally, it all looked even sadder:

- **Sony BMG rootkit scandal** . Epic EPIC FAIL. A long time ago in Galaxy Fair, Fair Await in 2005, Sony BMG was secretly stamping compact discs containing:

    1. Various crap like MP3, porn, etc.
    2. Built-in dREME - Extended Copy Protection with player and other crap
    3. SUDDENLY, rootkit

        Naturally, no one except Sony knew about the last point and, as usual, at first the buyers were extremely happy. But after the Jew Mark Russinovich tore off the covers, everyone was overcome by wild butthurt. The situation was aggravated 100500 times by the fact that

        1. Firstly, the system driver together with the rootkit was secretly installed and could not be removed at all.
        2. Secondly, on top of everything else, it was also full of holes. This was certainly taken advantage of by virus writers, who were beside themselves with joy that had fallen on their heads and subjugated the driver's functionality to their needs, gently but powerfully.
        3. Thirdly, the rootkit somehow contained the LAME Encoder code. It turned out that Sony itself violated someone else's copyright.

        In short , after many tons of beatings from the active public, Sony gave all the rootkit buyers normal disks with MP3 and even $7.5 in addition (http://news.bbc.co.uk/1/hi/technology/4424254.stm) . But the adventures with rootkits did not end there.
        And with the help of this rootkit, you could cheat and bot, for example, in World of Warcraft , simply by adding "sys" to the beginning of the name of the cheat's exe file.

- **GTA IV** . The protection (SecuROM version 7.35), into which Take 2 Int. spent not two or three, but much more millions, was broken in two days by some simple dick. The point is that Rockstar sawed a file with a bug that occurred in case of hacking - a drunk camera and uncontrolled forward movement appeared. And this did not prevent them from simply deleting the malignant tumor. And having installed some cracks, it was impossible to use the in-game Internet. As it turned out, the essence of the multi-million SecuROM protection was not even in copy protection, but in modding protection. And we are not even talking about replacing car models and their characteristics (although there is some kind of protection for this), but about protecting the program code of the

game. Replaced one byte in the exe (and it does not matter which one) - the game will not start, run the game with IDA enabled (and I don't give a damn that even the base is not GTAIV.exe) - fuck you. It gets to the point of absurdity, you can't even rename LaunchGTAIV.exe (even if it's a crack). With each launch, all exe addresses are recalculated, which makes debugging quite difficult, although the game is more lenient towards weak computers and doesn't get so sophisticated. The protection, of course, is not cast-iron, but it will give you a headache. The only question is, why the hell did Security make this perversion? Apparently, the brains of Security bosses remembered the scandal with SA's Hot Coffee and decided that the game should be protected first and foremost from modding, and not from illegal copying, and Rockstar probably didn't even bother to check Security's stuff.

- The Freemasons from **Electronic Arts** . They sucked up tuna after they received a class action lawsuit from users regarding the presence of a Trojan in Spore and a couple of other games that were protected by SecuROM. After the shitting out of bricks and a fucking amount of gold shekels spent on buying whores, cottages with gardens, Mercedes, yachts and other crap for honest judges and prosecutors, the top officials of the EA scam suddenly came to an interesting conclusion that it would be much cheaper for them to tell Sony DADC AG (https://archive.ph/6dMQs) to fuck off. After this incident, Sony lost the desire to shove Trojans/rootkits into its products, which cannot be said about the star-struck imbeciles.

- **Witcher 2.** Marcin Iwinski [3] spent a couple of hours after the game's release pulling porn from this internet of yours and simultaneously surfing various sites . He suddenly discovered that good pirates had already managed to crack the game and put it up for everyone to see (and, oddly enough , GOG's DRM-free version on torrents turned out to be of no use to anyone). After much frustration , Marcin and his superiors had their eyes opened, including the third one, and it was announced that DRM was evil and they no longer needed SecuROM.

- **Crysis** (SecuROM 7.34). Due to haste, the protection was installed crookedly, as a result of which it was hacked in a couple of days.

- **Crysis 3** (SecuROM 8). The magic of numbers in action — SecuROM was cut out after 3 days.

- **FarCry2** . A certain Yankee Adrian Kingsley-Hughes, having a serious excess of capital and a profound lack of intelligence, bought **a licensed** copy of the game, inserted the disk into his alien laptop, installed and launched it... and no fucking way! Secur rolled out a message to him that, supposedly, you, Adrian, are a loser, your cunning plan has collapsed and in general you won't fool Reinhard, because the disk in your drive is a backup copy. The patient is indignant and drools abundantly, because he didn't realize on his own that you can steal FarCry2 from a torrent **absolutely free of charge** .

- **BioShock** . To help the starving developers get at least some pennies from sales, Sony DADC AG decided to steal (from the office of *ActiveMark*) and immediately put into action a new feature: online activation. The **paul.dll** file (pasha.dll) was shoved into the game folder, through which an Internet connection was established with the Sony server for activation. Beforehand, the gullible user entered unknown runes like *J3QQ4-H7H2V-2HCH4-M3HK8-6M8VW* . But, firstly, no one thought about users without this Internet of yours - Blaukovich initially didn't give a shit

The essence of the problem
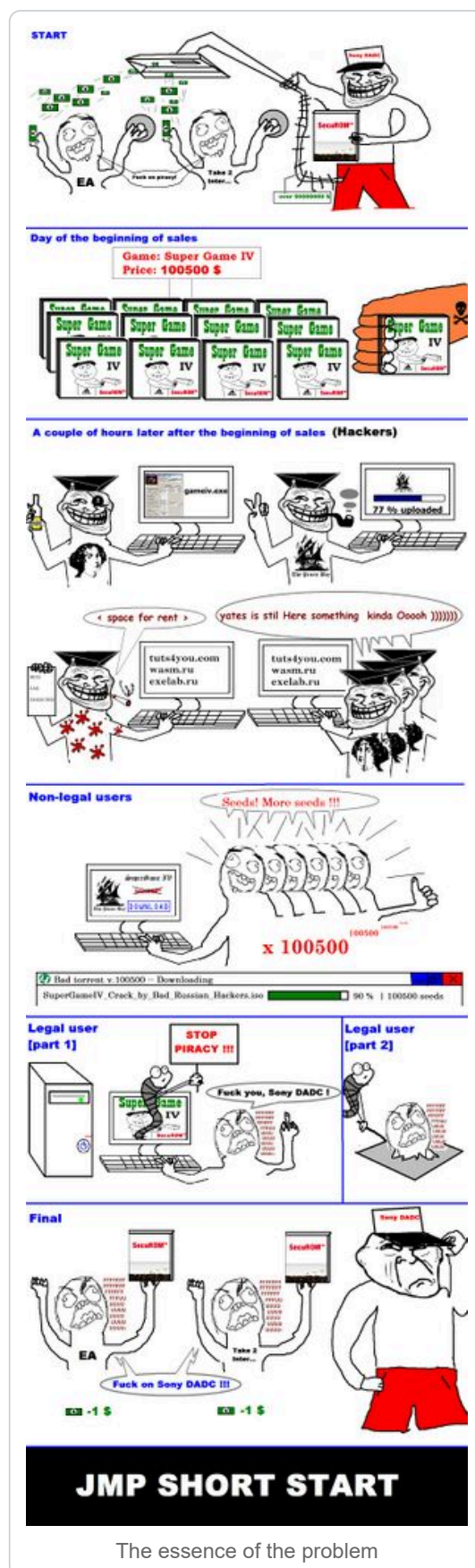
how they would be able to activate a piece of plastic with ones and zeros bought for five rubles. Secondly, there were still enough users with the Internet for the activation server to crash in the first hours of the influx of still happy buyers. Sony later justified itself by saying that the admin rebooted the server in rage after he himself could not activate Bioshock. Thirdly, there was a link to the hardware configuration of the law-abiding user's computer. And if the security guard spotted that the configuration had changed (for example, the user bought a couple of strips of pirated Corsair Dominator RAM), then he screamed about it over the network directly to Bla-Blah-Blaukovic. And finally, fourthly, the Austrian guys managed to valiantly step on a similar rake three more times.

- **Batman Arkham City** . And again the axe had a hardware binding, and even with a limited number of activation attempts (oddly enough). Even with a small upgrade of your computer, the stinking Batman had to be activated again. After the activation limit simply ended (accordingly, it is no longer possible to play Batman) - the butthurt of the unfortunate buyers reached astronomical heights. The most enchanting thing was that the activation cannot be restored , and what to do next - even Reinhard himself could not say. A fail of the most fucked up kind.

- **Dragon Age 2.** The above-mentioned sewing studio "Electronic Arts" has screwed over gullible users: first, the creator of the game BioWare (whom EA bought lock, stock and barrel) spread a rumor that they didn't need SecuROM . However, upon the release of the game, it turned out that everything was quite the opposite (https://archi ve.ph/CT3Xx) . Fans of the game felt a surge of happiness !

- **Final Fantasy VII** . Epic fail. In August 2012 , a la the end of the world, a re-released version of Final Fantasy 7 was released and ... I immediately went back. The reason is a bit banal - judging by the internal structure of the guts of the online activation of the security, the publisher mixed up the private RSA key for decrypting the HWID, and the users all went to hell.

- **paul.dll** . It is also *SecuROM PA (Product Activation)* . Some antiviruses recognize this file as a virus and immediately delete anonymous users from the computer. As a result, the subject refuses to start . Also, contrary to popular belief, the unlock code verification algorithm is located in a protected .exe file, and pasha.dll simply plays the role of a candy wrapper, from which you can only get return codes for correct/incorrect activation.

- **Sony DADC SecuROM version 8** . By and large, the hacker community has had enough of the new version of the subject ~~beer~~water and keeps silent. But the elves are already hinting that *the 8th version = simplified SecuROM 7.35* . No comments.

It's SecuROM

<blockquote>
« *Stop dumping VM's! Save the whales!* »

— **In the crack for GTA IV from Razor 1911**
</blockquote>

In addition to interesting technical solutions at the application level, there are lulz from developers in a separate line. The ASCII phrase **It's SecuROM** is used for identification and is present in a special encrypted data block. For crackers, the profit lies in service information about the current version of the subject and its features. The block is embedded in the main executable file and is located in the PE header.

Trolling hackers

The first thing that impudent hackers encounter when they mercilessly try to reverse engineer the developers' machine code is philosophical phrases (**AND DWORD PTR DS:[EAX], EAX** machine code, ♂ ☻ symbols ♀ ☺), which exist as text strings in ASCII format. Essentially, a meaningless set of letters and symbols, but with a special meaning:

- **< space for rent >** (correct Russian translation: *advertising space for rent*). Until a certain time, the most canonical phrase in the subject of version 7. It was shoved into the very beginning of the virtual machine (VM) and frankly delivered. According to persistent rumors, two unknown to science crackers took this lulz seriously and wrote a letter to Sony DADC asking to buy an advertising space for a tidy sum and replace the inscription with *"Vasya and Petya were here! Write to us: Vasya@mail.ru , Petya@mail.ru "* . Sony DADC, deeply shocked by what they read, were frankly offended and in the next version the phrase was replaced with the banal "You Are Now In A Restricted Area".

By the way, the virtual machine played a cruel joke on its developers: the presence of the VM was in the hands of hackers, since through it, like through an avenue, one could get into the OEP . As a result, the entire process of obtaining a dump was easier than pissing two fingers after a 1.5-liter bottle of Ochakovsky, which could not but please all the hackers.
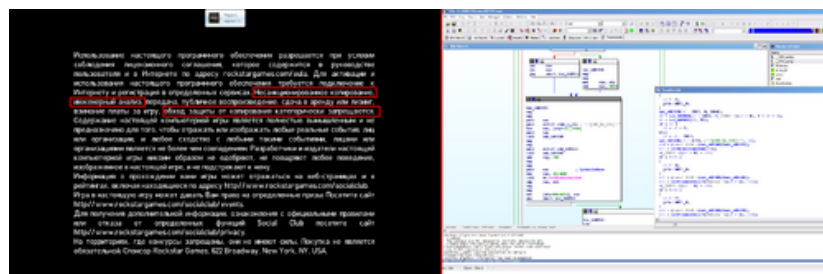
You won't believe it, gentlemen! I'm breaking and crying, breaking and crying...

- **yates stiiL Here kinda Ooooh** (correct Russian translation: *Yates is still here, like ooooh*). The phrase was also detected in VM. According to dead rumors, Yates is either a pet dog or Reigard's cat. People close to the developer circles claim that Yates is a real person, a pretty smart programmer who came from a cracker environment. The point of trolling was the ability to tear VM off the toy, which is the height of hacking especially complex protections.

- **The virtual machine is what it is** . Actually, its execution, of course, caused a lot of lulz. The whole dilemma is that any VM by its nature works very slowly . Because of this, all machine developers follow the following beaten path:

  1. Sawing of the general frame of VM
  2. Correcting your mistakes
  3. Adding whistles and gimmicks
  4. Correcting your mistakes
  5. Adding code obfuscation
  6. Correcting your mistakes
  7. *"F-ck!!!! The game started loading in a really fucking long time, instead of 20 seconds. Bitch! Fucking pump! We need to do some optimization."* [4]

And then at the last moment a frantic search begins for what needs to be simplified and what needs to be thrown out of the virtual machine! In the 7th security it looked like this: there were exactly 255 primitives of the VM machine code, and all of them had to be protected by code obfuscation... But old Reinhard was cunning and betrayed: in order for the virtual machine to work faster, the 2 most popular primitives contained completely open, "clean" code, which was unhindered. Using this fact, it was possible to make sure exactly how this virtual miracle works, and in the end, rip it out of the protected program to the Austrian wilderness, getting a fresh NoCD/NoDVD.

- **† MOV EAX, DEADC0DE** († *Dead code*). There were some fun twists with machine code, too. In the 16th numeral system, the number 0xDEADC0DE looks like the English phrase **Dead Code** , which literally translates into Russian as *dead code* . The trick is that the rest of the machine code that relates to this instruction is essentially dead garbage, meaning that the developers of the subject are playing the role of the great Captain Obvious.

- **Magic Byte** . After the first builds of the 7th version of SecuROM were released on cracker forums, some people who had been inside this Klondike of assembler artifacts began to whip up a feeling of the end of the world and horror, claiming that it was possible to hack the protection by tweaking just one magic byte. The community immediately split into three camps: the first said that the crackers themselves had gone nuts, the second expressed the opinion that Sony Dadz had gone nuts, and the third didn't give a shit from the start. It is not known for certain how it would have ended if the DAERM developers had not participated in squabbles on crack forums, since the next SecuROM build immediately reduced the degree of inadequacy on this issue. It seems that there was a hole, but it was patched up.

Snail joke

As it turns out, starting with version 8 ' you don't have to use a browser to access anedotsru . Whole jokes right in your debugger - innovation , huh!
The most famous one is about a snail in a bar: A snail walks into a bar and the barman tells him theres (there's).a strict policy about having snails in the bar and so kicks him out. A year later the same snail re-enters the bar and asks the

barman,.«What did you do that for?.)" .

Obviously , starting with version ^{9} , audio recordings of Misha Zadornov's concerts will definitely be added to the *.securom* section .

Copying code from SafeDisk

Not long ago, another interesting paradox was revealed - some pieces of the machine code of SafeDisk version 4.x and SecuROM 7.3x are almost completely similar. Since SafeDisk 4 was released much earlier (2005 from the first arrival) than the seventh version of SecuROM (2007 from the first arrival), the conclusion suggests itself that Sony DADC did steal the source code. However, there is information that the two companies entered into an extramarital union against the StarForce-SolidShield union [5] .

However, it is quite reasonable to assume that all the developers of DeRьMa are themselves engaged in reversing the products of their competitors in order to see what new things they have come up with, so that they can then steal them for themselves. Serious business is so serious!

Pirate disk in the drive, as if it were licensed

In early March 2013, information appeared that our super mega crackers were learning... learning , and, by the way, they actually learned how to patch the subject without Alcohol, Daemon Tools, or even without the original disk , so that it would recognize the left pirate disks from the bazaar in Mukhosransk as real licensed ones, which are illegally stamped by Sony DADC AG! Let's stock up on popcorn.

Keygen for online activation of SecuROM PA

YES! Another wild epic win: after the Chinese hacked Denuvo, an unlock code generator was announced on the cracklab website . Online activation consisted of generating an unlock code using **DES** (three variants) and **RSA** (the last HWID check) cryptoalgorithms. Part of the code was borrowed from the OpenSSL project. The request unlock code contained the HWID and the hash of the toy's individual DES key blank. The generated unlock code consisted of two parts - a service structure and an HWID.
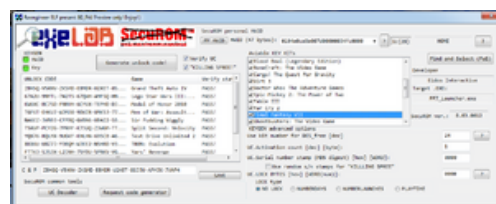
The official website for online activation of Securom is now no longer needed .

To the delight of anonymous users, it finally went public on January 17, 2016. It covered all the games protected by SecuROM with a napalm at once, requiring online activation. IN FACT, one clear library (born in 2012) covers such games with "napalm", which, when thrown into a folder with a greyhound toy, completely prevents the appearance of the activation window and, attention, the SecuROM disk request without any fuss with the keygen. Anonymous has already tested it on three titles, and this is only the beginning. That's it.

BigFish games

The biggest sucker in using SecuROM online activation technology was the American company Big Fish, which churns out PC trash using the shitty Adobe Flash technology . The Yankees bought SecuROM version 8.03.12 with the ability to activate Trial mode. SecuROM's Trial mode is slightly different from the traditional activation method, in that the activation itself is performed strictly through the server. However, there is a brilliant plot to break Trial mode:

1. We replace the current new version *of paul.dll* (usually v2.x) in the toy directory with the ancient version *of paul.dll* (v 1.x)
2. We get the option of "Manual activation" **!**
3. We use 80_PA keygen
4. Resetting the LOCK bits in the service structure
5. Generate a free unlock code
6. Insert and activate
7. …
8. PROFIT!!!

However, experienced crackers have long been aware that due to the underdevelopment of this Trial mode, you can do without a keygen: the control function in *paul.dll* should simply return **1** (one). Naturally, this can be achieved by simply using any debugger.

The SecuROM Trial mode is finally drowned by the fabulous stupidity of the BigFish developers themselves: unaccounted for features of launching Adobe Flash applications! Paradoxically, the main .exe application of any released PC game was a simple wrapper that, with the help of a simple command line, launched the interpreter. The latter, naturally, was not protected by SecuROM! Needless to say, in this case, the crack for trashy PC games from BigFish was written in TWO minutes at the MAXIMUM.

Fun fact: the Russian-language site BigFish offers ONLY games for iPhone , iPad and iPod touch. There are no PC versions of crap games with security , which kind of hints.

Error codes and workarounds

Error code (indicated in brackets)	What does it mean?	How to get around
1000	Remove the backup disk	**To screw up the Securo** disk geometry check by patching 3 (three) times the code like this: - `FLD QWORD PTR DS:[11EDC78]` - `FSUB QWORD PTR DS:[11EDC80]` - `FMUL QWORD PTR DS:[14AC050]` - `FCOMP QWORD PTR DS:[1483098]` - `FSTSW AX` - `TEST AH,05 (        )`
2000	Debugger is detected via PEB (*IsDebuggerPresent*)	Always clear the BeingDebugged flag
2001	GetTickCount always returns zero	The essence is similar to the error code *8007.* Some plugins or noobs hiding the debugger hook the GetTickCount function, forcing it to always return zero (for example, with a typical banal addition **XOR EAX, EAX** at the end). Therefore, it is necessary to disable this feature and not touch GetTickCount at all, because the subject **does not** use anti-debugging techniques based on counting the execution time of the code (RDTSC, GetTickCount, etc.).
3000	Debugger is caught by hardware breakpoints	Patch the code from the SEH handler on the UD2 instructions *or* install the hardware after checking (the hardware check module runs 2 times at the beginning and 2 times after a successful disk check)
5000	Debugger/hacker tool (in 95% - Process Monitor) is detected via *FindWindow*	Patch *FindWindow* and always return minus one *or* change the name in the main window of your hacker tool, which the developers have already blacklisted.

5001	Debugger (in 95% - SoftIce) is detected via *CreateFile*	Patch *CreateFile* and always return minus one *or* find a coolhack extension for softays.
5002	Debugger/hacker tool (Process Monitor) is detected via *FindWindowEx*	Patch *FindWindowEx* and always return minus one *or* change the name in the main window of your hacker tool, which the developers have already blacklisted.
6000	Software breakpoints at the beginning of VynAPI	No need to put INT3 on the first/second instruction
6005	Similar to 13001, with the only difference being that for the code section (after final unpacking, before jumping to OEP) and a different algorithm (CRC32?).	No need to set INT3 in the checked places. For the rest of the straight-handed ones, we set a hardware breakpoint for reading/writing on the checked section, jump out on the counting algorithm, and immediately after RET we get to the trigger condition like: • MOV ECX,DWORD PTR DS:[EDI+ECX+0x13A] • CMP EAX,ECX
8002	Debugger is visible via *CheckRemoteDebuggerPresent* (sho in NTDLL)	Patch CheckRemoteDebuggerPresent, returning zero (correct me anon if minus one)
8007	Integrity check *IsDebuggerPresent* failed (returned check value changed [6])	Being a newbie in hacking, you patched *IsDebuggerPresent* with the instruction **XOR EAX, EAX** (when you can simply reset the BeingDebugged flag and not fuck around)
8011	The debugger is detected by *ZwQueryInformationProcess* (which is in NTDLL), the argument *ProcessInfoClass* = **7**	Patch *ZwQueryInformationProcess* . Return any shit except zero.
8019	The debugger is detected by *ZwQueryInformationProcess* (which is in NTDLL), the argument *ProcessInfoClass* = **31** (*0x1F*)	Patch *ZwQueryInformationProcess* . Return any shit except zero.
9000	**The dfe** *or* **dfa** file , which are used to decrypt data in the protected game's data files, is fucked up . SecuROM Data File Activation is to blame for everything, bitch.	Get files from the internet
10000	The debugger detects the name of the parent process.	Rename *ollydbg.exe* to *lurkmore.exe* etc. SND Olly, for example, does not suffer from this bullshit.
13000	The integrity of the protected .exe file has been compromised	SecuROM opens itself (.exe file) via WinAPI *CreateFile* , and methodically calculates the checksum in sections, reading bytes *ReadFile* . This can be broken in two ways: • The most common one, which has been used since the times of StarForce 3.x, when *protect.dll* had to be

stuffed with its own executable code. The original file *filename.exe* is copied and immediately renamed to some *filename_original.exe* . An interceptor is inserted into *filename.exe* , which throws a hook to *CreateFile* (which is in kernel32) and when the protection tries to open *filename.exe* , it makes a redirect to *filename_original.exe*

- Purely Securomovskiy. After *CloseHandle* opened *filename.exe* , the first instruction that comes up is edited:

  - ```
    POPFD... CMP EAX, 1 (
    ```

    ```
    )
    ```

| 13001 | The integrity of the file's PE header has been compromised. | In the vast majority of cases, the error occurs when trying to add new functions to the import table, for example via LordPE™ or PeTools™. SecuROM has a spare original PE header, which is compared via XOR with your patched one in 4-byte increments:

- `XOR ECX,DWORD PTR DS:[EDX]`
- `NOT EAX`
- `XOR ECX,EDX`
- `CMP EAX,ECX`

- `MOV EAX,EDX` |
| Whole line :
Conflict with Emulation Software detected | Crooked emulation of disk braking by this Daemon tool of yours. Fail when comparing the speed of a circle. | This unhealthy crap is typical for multi-core processors . If manually assigning one core to the target process in the task manager does not help, it is treated in the debugger: You need to find *DeviceIoControl* with the argument *IoControlCode* = IOCTRL_DISK_PERFOMANCE (0x70020). Usually this is a separate function located in a loop and started in a new thread, with active geometry checking. At the end of the loop, something like:

- `FILD QWORD PTR SS:[LOCAL.9]`
- `INC DWORD PTR SS:[ARG.1]`
- `FILD QWORD PTR DS:[12D1E80]`
- `FDIVP ST(1),ST`

- `FSTP QWORD PTR DS:[EDI-0xC]` |

In short , *DeviceIoControl* should return zero in **EAX** . Securo understands that it is impossible to check the speed and skips the module . Epic win!

Disciplines

It is quite obvious that security is the subject of squabbles in special disciplines, mostly arranged by journalists in their articles:

- **StarForce vs SecuROM** - which is cooler?
- **StarForce-SolidShield vs SecuROM-SafeDisk** - who's the faggot and who's the d'Artagnan?

The showdowns between the SkidROW (https://archive.ph/2uspC) *and* (https://archive.ph/2uspC)*RELOADED* (https://archive.ph/2uspC) *bandit groups* (https://archive.ph/2uspC) with the use of machine guns and grenade launchers are taking place separately .

OOO "Secur"

Also, in the vastness of independent Ukraine there is a company called "Secur", which is engaged (and what would you think) in the import of security gadgets . However, anon does not know whether it is controlled through Sony DADC offshores or by Reinhard itself.

DENUVO

Main article DENUVO .

A sad outcome

For over 10 years, DRM producers have been trying to combat piracy in this country! And what do we have at the moment:
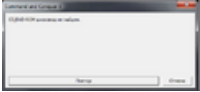
- DRM production is a business with its own blackjack and whores .
- Piracy is steadily growing every year.
- In most cases, the saying applies: "They should have protected their SecuROM first, then this GTA"
- Blaukovich did not save the world from unlicensed copies, and the future of his product is rather bleak.
- The Pirate Bay rules!
- Russian authorities are actively working to solve the problem along with the development of nanotechnology .
- for 7 months the peracute has been defeated. Crackers have been bought, Secura 9 (Denuvo) is broken not by masters, but by green snot, a teaspoon per hour. The second level of the food chain was allowed to earn some

money on activations. However, considering the fact that games of far from first, or even second grade were released on this protection , everyone except schoolchildren doesn't give a damn.

Gallery

Reinhard Blaukovich's Nightmare

Bitch!

OH SHI--

Amazon.com lost the key

Circulation of legal users in support

Schoolboy, are you downloading from PirateBay? You're next!

Fails. Thousands of them!

A rootkit, you say? Reinhard is hiding it!

Petrosianism of bourgeois journalists

Video

Hitler and the Secur

Hitler and Securo in GTA IV

Tiberium Reversal

A lulz sequel to Tiberium Reversal

Tiberium Reversing. Keygen for online activation
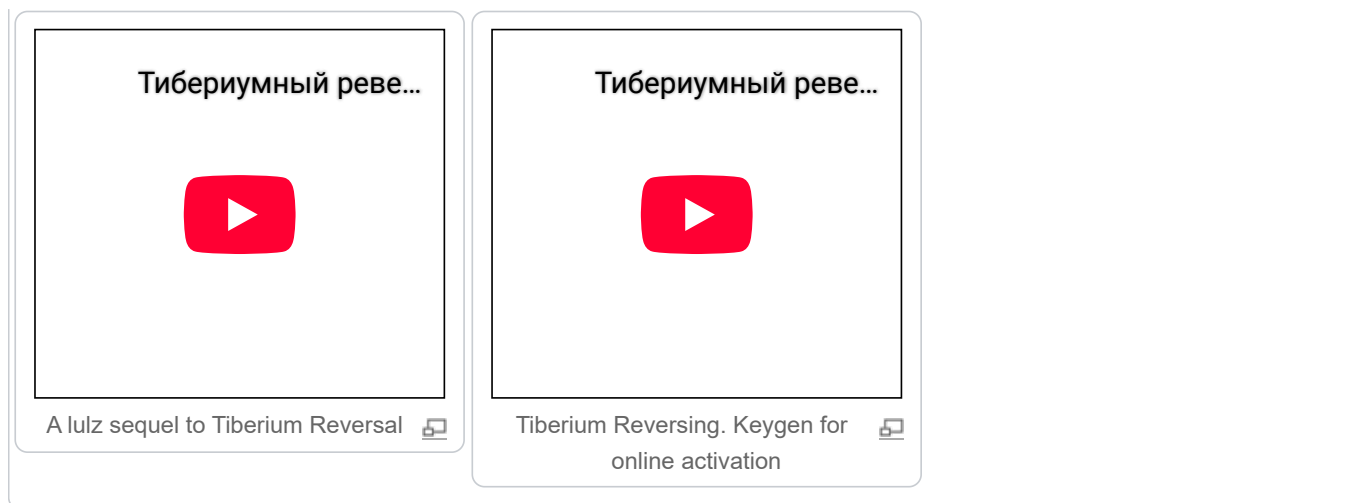
See also

- DRM
- StarForce
- Tablet

Notes

1. Although it would be a stretch to call it DRM, because by all characteristics the first generation was clearly inferior to the trio of SecuROM, SafeDisk, StarForce

2. Everything is open - I don't want to disassemble it. Reinhardt with his Securomus would have his jaw dropped from what he saw.

3. The founder of CD Projekt Red, which made the game

4. Exception: Starforce. Its crazy developers, on the contrary, only stuff in more garbage code and clog up the VM on a cosmic scale, because they are chronic idiots.

5. This is confirmed by the fact that Sony and Macrovision maintain the same "black list" of cracker software, which significantly spoils their products and spoils their own mood.

6. Yes! Yes! Dear Anon! Blaukovich also read Chris Kaspersky's books and is aware that *IsDebuggerPresent* simply reads the value of the *BeingDebugged* flag from the PEB structure. Accordingly, SecuROM first simply calls this function, and then SUDDENLY puts its own random number into *BeingDebugged* and checks whether it appeared at the output *of IsDebuggerPresent*

	These people are very interested in games, so	[collapse]
Meta	Video Games • Game Memes • Game Mods: A Good Thing or Not? • Game Tsakoldism • Open Labyrinth World • Drama Around the Russification of Sword Art Online • Hideo Kojima	
Genres	Аркада • Браузерка • Рогалики • Эроге • Порно-игры • FPS • RPG (MMORPG • MUD) • Rhythm game • RTS • TBS • Quest • MOBA • Онлайн-игры • Скурвившиеся игры • Клоны X-COM • Tower Defense • ККИ • Рандомайзер • Инди-игры • EXE (жанр инди-игр) • AyakaLounge • Gacha Life • Геймдев Афиша • Санчоус • Tabovri • Replayed • Polycount.com	

Платформы	Неигровые (PC • MSX • Спектрум • Amiga) • Консоли (Игры • Dreamcast • NES • PSP) • Steam Deck • Brick Game • Тамагочи • Игровые автоматы • Dance Dance Revolution • Pump It Up • Платформосрач • Unity Engine • Олег Керман • RTGame • Блокировка Twitch в России • IShowSpeed • Супер Вадимка • Доктор Кулик • Приключенческая игра • Стекло для монитора • Геймергейт привёл к победе Трампа • ShadowPriestok • Все игры — стрелялки • Иван Дипинс • Амазинг Онлайн • Скорость улучшения графона
Корпорацъи	1C • 3dfx • Адамант Мультимедиа • Акелла • Иннова • Нивал • Фаргус • BioWare • Blizzard • Ice-Pick Lodge • Neogame • Nintendo • Sony DADC SecuROM • StarForce • Steam • Type-Moon • Иксолла • CD Projekt RED (Закончили как настоящие поляки) • Tencent • Steam • NetEase • Exorsus • Blizzard Entertainment • Gas Giant Games • Paradox Interactive • Arizona Games • Bethesda • FromSoftware • Sweet Baby Inc • Metro Videogaming Entertainment • Rockstar London • Rockstar Vienna • Rockstar Vancouver • Rockstar San Diego • Rockstar India • Gameloft • Electronic Arts • Ubisoft • Виктор Павлов (ViteC ► Play) • Антон Татыржа (T2x2) • Глеб Орлов (Sasavot) • Mazellovvv • PPSSPP • Wings Gryphons
Особенности	10 заповедей геймдева • Alignment • Dungeons and Dragons • Hit-and-run • One-liner • PunkBuster • Жестокость в компьютерных играх • Классические игры для DOS • Компьютерный клуб • Корейская система крафта • Машинима • Метод Мартингейла • Оружие в компьютерных играх • Пасхальные яйца • Пиратские игры девяностых • Рандом • Русефекации • Мобильные игры • Летсплей • Продажа аккаунтов в видеоиграх • Баланс (видеоигры) • Микротранзакции • Энергия (мобильные игры) • Режим Ironman • Serana Dialogue Add-On • Поражение • Ранний доступ • Игровой стаж • Правила игры • Быстрый геймплей • Пиратский сервер • Игра как сервис • Обход блокировки • Уродливые персонажи в играх • Unreal Engine • Havok Physics • Винрейт • Desire sensor • Vinesauce • PARI X BRFF CS2 2023 • GAMEDEV CITYFEST 2024 • Феномен жёлтой краски • Деревянная парочка • Hier spielt Vielfalt • Игровое кресло • UE-сектант • Систем-селлер • Unreal Engine 5 • Индекс деревянного ящика
Термины	Barrens chat • Powerleveling • Spectator • Босс • Геймерский сленг • Донат • Фарм • Ебай • Жаргон MMORPG • Жаргон MUDаков • Искусственный идиот • Кемпер • Мультоводство • Отыгрыш • Плюшки • Твинк • Фаербол • Фарминг • Читер • PC-гейминг • Кат-сцена • Симуляция жизни • Тильт • A-Life • Incorporated • OG Loc • Type 59 • M19 • New Game+ • Имба • Power creep • Нерф • MMR • Античит • Автобаттлер • Ладдер • Пинг • Челлендж • Софткор • Рестарт • Десинк • GG • Дюп • Гильдия • Хаб • Один ХП • Финишер • Эндгейм • Свиток портала • Уровень сложности • Быстрое сохранение • Автоподбор предметов • Танк (видеоигры) • Currency sink • Цифры урона (видеоигры) • Геймификация • Дверь измерений • Два монитора • Стрим-марафон • Реклама мобильных игр • DLC • Free to play • Лутбокс • NPC • PvP • Агро • Микрочел • Ремастер • Нубик • Фидить • Взрыв трупа • Вихрь • Мелкоуправленчество • Ретрогеймеры • Душнила • Киберспорт • S1mple • Вархаммер-словарь • Меткий глаз • Босс фотографирует • Тяжёлый перекат • Боссы Vanilla Plus • Честное прохождение Souls-like • Распродажи в Steam • Игра в группе • Одиночная игра • Уровень Steam
Геймеры	**Геймергейт** • Kindly Miquella • Биллибой • Геймер • Железнодорожный симмер • Задрот • Казуал • Манчкин • Мариобой • Симмер • Сонибой • Тракторист • Казуал • Вхале • Подпивас • Ума (Ведьмак) • Wheelman • Папич • Рандом • Баттлпасс • Соникофан • Игровая импотенция • Коуч по видеоиграм • Itpedia • BalphaGore • Алексей Фингерут • Бабай Великолепный • TyutcheV_V • Михаил Афанасьев-Гредескул
Персонажи	Конкретные: Bridget • Декард Каин • Dopefish • Earthworm Jim • I.M. Meen • Slenderman • Sonic the Hedgehog • Uboa • Айрис • Артас • Дирижабль Киров • Император Человечества • Индиана Джонс • Кейн • Лара Крофт • Мамонт-танк • Марио • Солид Снейк • Сырно • Тали • Неизвестный полубог (Elden Ring) • Маления, Клинок Микеллы • Пудж • Цирилла • Моргонет (Grim Dawn) • Марика (Elden Ring) • Патчес • Кейра Мец • Довакин • Лоуренс, Первый Викарий • Людвиг Священный клинок • Герман, Первый Ловчий • Нейрелла • Радагон • Дрочеслав, сын Сергея • Явгмот • Рыцари горнила • Моргот, Король знамений • Двойные боссы (Elden Ring) • Маления Без Примесей • Генерал Радан • Маликет, Чёрный Клинок

	Собирательные: Вампиры • Зомби • Паладины • Орки • Роботы • Золотой порядок • Древо Эрд • Босс • Треш-монстр • Гоханц Чернейший • Херобрин • Капитан Прайс • Лут гоблин • Босс-паук • Green Hill Zone • Мясник • Баал • Босс-вертолёт • Охотник на ведьм (Disciples II) • Лобстермен • Никсы • Эльфы • Лазурный дракон • Эфириалы • Alina Gingertail • Микелла Милосердный • Чёрный самурай в Assassin's Creed: Shadows • Дилемма Партурнакса
Люди	Angry Video Game Nerd • Boomer • GamerSuper • Levelord • Илья Мэддисон • SupLisEr • Twixt • Yahtzee • Aeгоров • Алевиус • Американ МакГи • Ваномас • Врен • Гульмэн • Кармак • Номад • Петрик • Роммель • Сир • Ставицкий • Шульц • Мамкодолбы • Sir Troglodyte • Нуб • Уголок Твистера • Ролевики • Adolf RA • Джон Кармак • Гейб Ньюэлл • Патрик Ламберт • Дмитрий Кунгуров • Gangena • Доширачник • Тоха • Гейм-мастер • Kalcor • Sam Mason • Антон Александров • Михаил Мирчук (Майкер) • АнтикварЪ-Гейминг • Крис Уилсон • Иван Гамаз • Бобби Котик • Дмитрий Глуховский • Габен Ньюел • Docent Picolan • Mahadev • Xatab • Дядя Обрящиков • Гулаг (GameDev) • Ozon671games • Дэниел Петрик • BartGameTV • Pixel Devil • Абдуль • Agafonoff • Таганай • Максим Пилипчук • Дмитрий Аскаров • Серёга Пират • FreddieW • TheBrianMaps • Графодрочеры • Natrezim • Grummz • Хидэтака Миядзаки • Nomad Bones • Нагибатор • Эдмунд Макмиллен • Роман Артеменко • Оборотень
Сообщества	GameDev.ru • DTF • GoHa.Ru • Half-life.ru • Prodota.ru • Twitch.tv • Vg • Outland • GoodGame • Sc2tv.ru • Watch Dogs vs GTA 5 • Discord • Nexus Mods • Glasscannon.ru • RMT (Ownedcore • EpicNPC • Mulefactory) • RetroAchievements.org • D2jsp • DF2 Forum • BasedMods • San Andreas Multiplayer • Game item auctions • CBBE • Obsidian • Dacha production • Game Open Lab • DRЫNDA • Xbox Ambassadors • Sosnuli • Discord blocking in Russia • Story runner syndrome
Game Journalist	Printed (Game.exe • MegaGame • Great Dragon • Virtual Joys • Land of Games • Igromania • Xakep • LKI • Navigator) • Online (Playground.ru • StopGame.ru • Zero Punctuation • Ag.ru) • Let's play • Off to the beat • Physics of the World of Heroes

A very useful thing, allows machines to work with commands.	**[expand]**

Pirates are always ready to make a proper robbery	**[expand]**

Covered in shame forever - do not allow artists into power	**[expand]**

Источник — https://neolurk.org/w/index.php?title=SecuROM&oldid=1740557

Add your comment

On the site Neolurk, the people's Lurkmore **all comments** are welcome . If you do not want to be anonymous, register or introduce yourself . It is free.

[ ] I'm not a robot
reCAPTCHA
Privacy - Terms

[Leave a comment] [Preview]

Sort by date ▼   Enable automatic update of comments

This page was last edited on 12 May 2025, at 12:24.

Сайт может содержать мате

This page has been accessed quite a few times.