SecuROM — Lurkmore

БЛДЖАД!

Эта статья полна любви и обожания.
Возможно, стоит добавить немного критики?

ACHTUNG! Опасно для моска!

Министерство здравоохранения Луркмора предупреждает: вдумчивое чтение нижеследующего текста способно нанести непоправимый ущерб рассудку. Вас предупреждали.

«Если ассоциировать SecuROM v7.33.17 с танком Абрамсом без динамической защиты, OllyDbg — с гранатометом РПГ-7, а X-code injection — с кумулятивной гранатой для гранатомета, то как и в реальности, такой выстрел навзничь прошьет броню этой тяжелой и неповоротливой машины и достигнет цели — OEP. Выведенную из строя машину изучают Российские инженеры… »

— *Тибериумный реверсинг*

†**SecuROM** (*секуром, секур, секира*) — защита от копирования злыми пиратами и праздношатающимися хакерами этих ваших игр, музыки и всей прочей хуиты®, защищенной авторскими правами™ и распространяющейся на электронных носителях. В отличие от сраного говноStarForce™, любима хакерами и поэтому известна своей низкой взломоустойчивостью: по дефолту взломанная версия появляется на торрентах максимум дня через два, в худшем случае — через пару часов. По аналогии с двумя предпоследними версиями Windows, крекерами наиболее почитаема линейка **7**.3x, в том время как последняя, **8**, версия является копией 7.35 чуть менее, чем полностью. На планете Земля сие творение выпускала буржуйская контора Sony DADC AG(на гуглоспутниках), которая кроме штампования CD/DVD болванок решила срубить бабла прежде всего с известных студий aka жадных разрабов, и что самое интересное — таки срубала, но с кряхтением и скандалами. В конце концов, в 2013 году успешно похоронена нашими хакерами с *cracklab*… чтобы уже в 2014 году, как крисалид, вылупившийся из зомби, возникнуть в виде форк 7 версии сабжа — *DENUVO*.

Появление на свет

В далеком 1999, когда жлобы буржуйских контор по производству наркотиков для игроманов начали потихоньку охуевать от распространения пиратства в этой стране и прилегающих территориях, ВНЕЗАПНО, откуда ни возьмись, объявился некий австрийский жыд Рейнгард Блаукович. Под предлогом вломить пизды распоясавшимся хакерам он предложил Sony DADC создать новую защиту для игровых контор и издателей. Идея была воспринята Sony на ура, поэтому Блаукович быстренько сколотил команду разработчиков, придумал название системы защиты и начал потихоньку продвигать сабж в массы.

Дизассемблировали, развалили и потанцевали на крышке гроба.

Блаукович в печали — прочел до конца «Тибериумный реверсинг». Канонічное фото

«С любовью, Electronic Arts и Take 2 Interactive»

Разработчики уже обсуждают следующую версию

Примета: Рейгард пробует себя в большом спорте — разрабов SecuROM скоро выставят на мороз

LEGO Рейнгард™ смотрит на тебя, как на жертву копирастии

Больше спортивного Рейнгарда Блауковича

Trollface

Bruce Lee

Solid Shield, SafeDisc, SecuROM

Щас вдует

Танцует

Увидел свою руку

Причины любви

«Британские ученые доказали, что если Ваша игра защищена SecuROM, интерес крэкеров к ней возрастает в среднем от 101 до 200% »

— Британский анонимус

Довольно банальны:

Ну что тут еще можно сказать...

- Разреверсив SecuROM, можно много чему научиться и перенять, ни разу при этом не блеванув от говнокодинга. Дело в том, что в отличие от некоторых отечественных звезданутых, разработчики сабжа не страдают параличом верхних конечностей, арбидальной дисфункцией головного мозга, аннигиляцией глазных нервов, зашкаливающим самомнением и другими проявлениями криворукости.
- В каждой версии есть что-то новое.
- Приколы inside.
- Целые анекдоты в поздних версиях.
- Дружелюбный юзер-интерфейс от **drm_dialogs.dll**
- Сабжем защищаются, как правило, самые широко известные проекты (GTA, Command & Conquer, BioShock, Witcher, WarCraft III, FarCry 2).
- Эффект от первого взлома обязательно доставляет неимоверный экстаз всем участникам (крекеры, разрабы, издатель, простые юзеры), а %nickname взломщика обязательно отмечается интернет-общественностью и даже в новостях.

- ???????
- MOV EAX, DEADC0DE

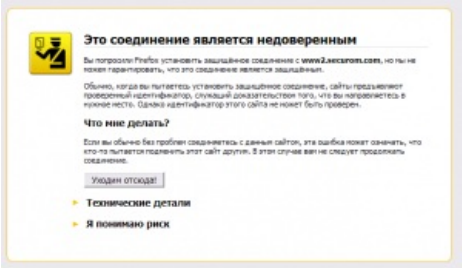
Объяснение одной цитатой

«Сравнить SecuROM и StarForce, абсолютно тоже самое, как сравнить Volkswagen Passat CC(SecuROM) и ВАЗ-2105(StarForce). Если первый делали действительно профессионалы, с учетом всех рисков, то разработчики второго - обычные троечники, которые кроме книги Рея Данкана "Профессиональная работа в MS-DOS" ничего не читали. Поэтому после того, как Sony признала свою неправоту в отношении захвата нулевого кольца операционной системы и отказалась от него, разработчики старфорса, на зло всем, держатся за ядерный уровень, как за мамкину юбку, ибо жалкий IsDebuggerPresent в засратом protect.dll заставляет смеяться даже начинающих взломщиков. Настоящая DRM - очень сложная система, которая ни в коем случае, не должна мешать легальным пользователям, но в то же время, как защитное покрытие от коррозии - на максимально возможный срок огородить целевую программу от рук пиратов; а не руткит или троян, который контролирует все действия конечного пользователя и показывает BSOD, если ему что-то не нравится. »

— ТруЪ-изречение на одном из андеграунд-форумов(Говорят: ©Крис Касперски)

SecuROM в России

В этой стране мало что известно о секуроме и вообще Сони Дадц, поэтому бытует только один миф, что якобы SecuROM является херовой защитой и ломается быстрее, чем продукция АвтоВаза. На самом деле данный миф активно пропагандируется в журнализдских статейках, авторы которых были куплены с потрохами Protection Technology и теперь на каждом зассаном углу воспевают величие отечественного производителя. Дело в том, что все известные большие студии (Electronic Arts, Take-Two Interactive) по штампованию игр находятся на Западе. Последний, имея развитое законодательство и здравый ум, просто послал нахуй этот звездный высер и сказал его авторам катиться ко всем чертям, тем самым даровав возможность пылесосить бабло с издателей игр только Sony DADC, подельщикам из Macrovision Corporation, ну и чуть-чуть лягушатникам с их унылым солидольным щитом. В общем, мечта о сотнях нефти и всемирном призвании у ребят из Protection Technology рухнула.



Огненная лиса не рекомендует шляться по сайтам DRM-производителей!

Впрочем, пик дэрэмизации пришелся на 2005—2009 г (2007±2 г.), и после продолжительной серии фэйлов Рейнгард начал понимать, что не за горами тот час, когда на SecuROM наденут деревянный макинтош, и в Sony DADC AG заиграет похоронная музыка, но сабж ее не услышит. Чтобы хоть как-то спасти ситуацию, была запилена дружба с каким-то филиалом ZOGa под названием Tribeka. Однако статистика неумолимо показывает, что сабж уже не торт и потихоньку скатывается с винрарных Warcraft III, GTA, CnC, FarCry, MassEffect до защиты попсовой хуйни от студии Walt Disney типа Brave Video Game или Disney Princess: My FairyTale Adventure, которая предназначена для детей младшего возраста. Но как ни странно, современной молодежи такие игры и на хуй не всрались — их хлебом не корми, дай пострелять в Battlefiled 3 или Counter-Strike. Поэтому продажи детских диснеевских поделок держатся на нехороших хэкерах славянской национальности, которые покупают сие только из-за того, чтобы ~~поиграть~~ дизассасемблировать потроха новой версии секурома и

SolidShield

SolidShield-жалкие потуги сброда нубов, с идиостким названием Tages SAS и пидарастическим лого в виде голубого диска, нашкребсти бабла на пиво (а если заказ серьезный, то заодно и на дурь). Единственная DRM(?)[1], которую дизассасемблируют поржать ради. По виду - выкидыш старфорса: **protect.dll** переименовали в **hc.dll**, ИЧСХ говноразрабы StarForce явно приложили руку к запилу виртуальной машины, ибо все остальное на фоне VM ну просто обычный C++ код, откомпилированный в MS VC++ 7.0 [2]! Собсна сама VM была кошерной в первых билдах и ближе ко 2му едишину скатилась в такой же ебаный стыд, потому что тонкая психика програлмеров из Protection Technology треснула от издевательств

получить очередную порцию лулзов. Отака хуйня, малята!

Скандалы унд фейлы

крекеров и им стало глубоко по хуй-хуле, лягушатники хавают. Самый известный лулз был с первым Ведьком: в силу невиданного доселе распиздяйства, разработчики в солидольной щите забыли активировать функцию анти-отладки, несмотря на то, что сам код, отвечающий за детекд дебаггеров, присутсвовал. В итоге, сабж можно было дебажить хоть до полной усерачки. Справедливости ради стоит отметить, что встречается редко.

Локально всё это выглядело еще печальнее:

- **Sony BMG rootkit scandal**. Былинный EPIC FAIL. Э лонг тиме агоу ин гэлэкси фэр, фэр эваи в 2005 уеар Сони БЭМЭГЭ подпольно штамповала компакт-диски в которых содержалась:

  1. Разная хрень типа MP3, прона и т. п.
  2. Встроенная дэрэмэ — Extended Copy Protection с плеером и прочей херней
  3. ВНЕЗАПНО, руткит

  Естественно, про последний пункт никто кроме Sony не знал и, как обычно, поначалу покупатели были зело довольны. Но после того, как жыд Марк Руссинович сорвал покровы, всех постиг дичайчий butthurt. Ситуацию в 100500 раз усугбляло еще то, что

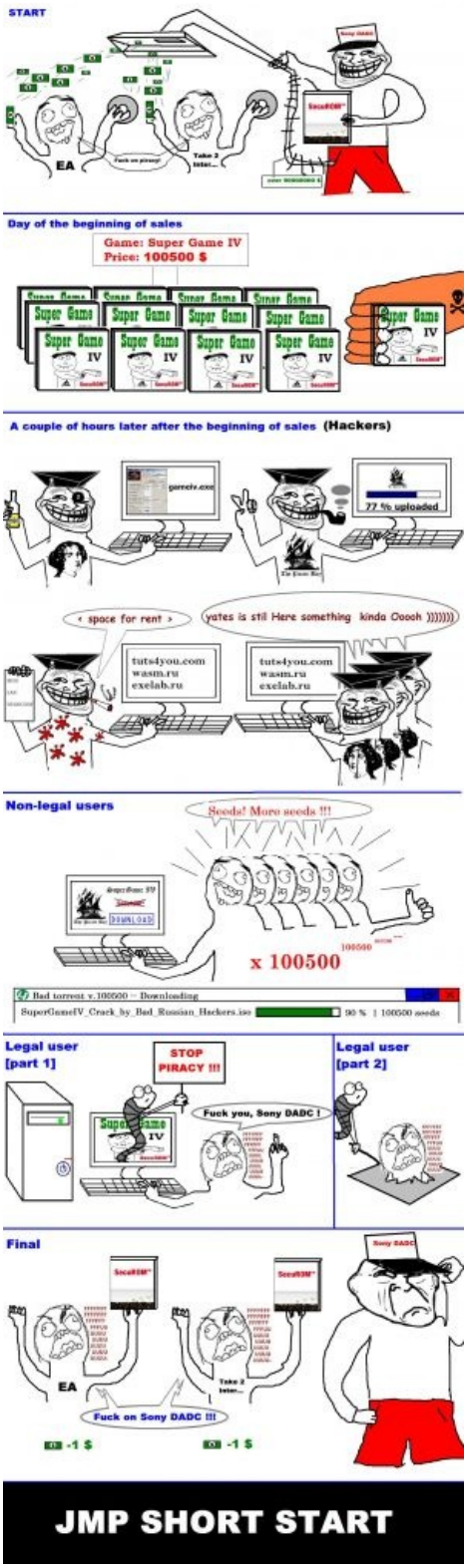
  1. Во-первых, системный драйвер вместе с руткитом скрытно устанавливался и вообще никак не удалялся.
  2. Во-вторых, ко всему прочему, он был еще и дырявым. Этим непременно воспользовались вирусописатели, которые были вне себя от свалившейся на их голову радости и подмяли функционал драйвера под свои нужды нежно, но властно.
  3. В-третьих, в рутките каким-то хуем присуствовал код LAME Encoder. Получалось, что сама Sony нарушила чужие авторские права.

  Короче, после многих тонн выгребленных пиздюлей от активной общественности, Sony раздала всем покупателям руткита нормальные диски с MP3 и даже 7,5$ в придачу. Но приключения с руткитами на этом отнюдь не закончились.
  А ещё с помощью этого руткита можно было невозбранно читерить и ботоводить например в World of Warcraft, просто добавив в начало имени exe-файла чита «sys»

- **GTA IV**. Защиту (SecuROM версии 7.35), в которую Take 2 Int. вбухала не два и не три, а намного больше миллионов, разломал за два дня какой-то простой хуй. Соль в том, что рокстары запилили файл с багом, который возникал в случае взлома — появлялись пьяная камера и бесконтрольное движение вперёд. И это не помешало просто удалить злокачественную опухоль. А поставив некоторые кряки, нельзя было пользоваться внутриигровыми интернетами. Как оказалось, суть многомиллионной секуромовской защиты заключалась даже не в защите от копирования, а в защите от моддинга. Причем речь даже не о замене моделек машин и их характеристик (хотя на это защита хоть какая-никакая но тоже имеется), а о защите

программного кода игры. Заменили один байт в exe (и не важно какой) — игра не запустится, запустите игру с включённой IDA (и похер что даже база не GTAIV.exe) — хер вам. Доходит до абсурдного, даже нельзя переименовать LaunchGTAIV.exe (даже если это кряк). С каждым запуском все адреса exe пересчитываются, что нехило так усложняет дебаг, правда к слабым компам игра относится более снисходительно и так не изощряется. Защита, естественно, не железобетонная, но геморра подкинет на голову. Спрашивается лишь нахуя секуром запилили сие извращение? Видать надмозг секуромовских боссов припомнил скандал с САшным Hot Coffee и решил, что защищать в первую очередь надо игру от моддинга, а не от незаконного копирования, а рокстары небось даже и проверять секуромовщину не стали.

- Жидомасоны из **Electronic Arts**. Лососнули тунца после того, как получили коллективный иск от юзверей на предмет наличия трояна в Spore и паре других игр, которые были защищены SecuROM. После высранных кирпичей и неебического количества золотых шекелей, ушедших на покупку шлюх, дач с огородами, мерседесов, яхт и прочей поебени честным судьям и прокурорам, верховные лица шарашкиной конторы EA внезапно пришли к интересному выводу, что им будет гораздо дешевле послать Sony DADC AG на йух. После этого случая у Сони закончилось желание пихать трояны/руткиты в свои продукты, чего не скажешь о звезданутых имбецилах.
- **Witcher 2.** Марцин Ивиньски[3] пару часов после выпуска игры тянул прон с этого вашего интернета и параллельно шастал по разным сайтам. Совершенно внезапно он обнаружил, что добрые пираты уже успели взломать игру и выложить ее для всех желающих (ИЧСХ, GOG'овская DRM-free версия на торрентах оказалась найух никому не нужна). После продолжительной фрустрации у Марцина и его начальства открылись глаза, в том числе третий, и было объявлено, что DRM — зло и SecuROM им больше не нужен.
- **Crysis** (SecuROM 7.34). Из-за спешки защиту криво повесили, в результате чего она была взломана за пару дней.
- **Crysis 3** (SecuROM 8). Магия чисел в действии — SecuROM выпилили через 3 дня.
- **FarCry2**. Некий пиндос Adrian Kingsley-Hughes, имея серьезный переизбыток капитала и глубокий недостаток ума, купил **лицензионную** копию игрушки, вставил диск в свой инопланетянский ноутбук, установил и запустил…да ни хуя же! Секуром выкатил ему сообщение, что, дескать, ты, Адриан, лох, твой хитрый план рухнул и вообще Рейнгарда не проведешь, ибо диск в вашем приводе является резервной копией. Поциент негодуэ и изобильно брыжет слюной, ибо самостоятельно он не доехал до того, что стащить ФарКруТу с торрента можно **абсолютно бесплатно**.
- **BioShock**. Чтобы помочь голодающим разрабам получить хоть какие-то копейки от продаж, Sony DADC AG решила самостоятельно спиздить (в офисе фирмы *ActiveMark*) и сразу бросить в ход новую фичу: online-активацию. В папку с игрой впихивался файл **paul.dll** (паша.длл), через который устанавливалось соединение по интернету с сонькинским серваком для активации. Предварительно доверчивый юзер вводил неведомые руны вроде *J3QQ4-H7H2V-2HCH4-M3HK8-6M8VW*. Но, во-первых, о юзерах без этого вашего интернета никто и не подумал — Блауковичу изначально было как-то похуй, как те смогут активировать купленный за пятихатку кусок пластмассы с единичками и ноликами. Во-вторых, юзеров с интернетом все равно хватило для того, чтобы сервак активации рухнул еще в первые часы наплыва пока еще счастливых покупателей. Sony позднее оправдывалась тем, что админ в ярости ребутнул сервак после того, как сам не смог активировать Биошок. В-третьих, существовала привязка к аппаратной конфигурации компа законопослушного юзера. И если секуром палил, что конфиг поменялся (к примеру, юзер купил пару планок пиратской оперативы Corsair Dominator), то вопил об этом по сети непосредственно Бла-Бла-Блауковичу. И наконец, в-четвертых, австрийские посоны умудрились еще три раза доблестно наступить на аналогичные грабли.
- **Batman Arkham City**. И снова секира имела аппаратную привязку, да еще вместе с ограниченным количеством попыток активации (как ни странно). Даже при небольшом апгрейде своего компа, вонючего бетмена нужно было снова активировать. После того, как лимит активаций банально закончился(соответственно играть в бемтена уже нельзя) — баттхерт горе-покупателей достиг заоблачных вершин. Самое феерическое было то, что активацию нельзя восстановить, и что делать



Суть™ проблемы

дальше — не мог сказать даже сам Рейнгард. Фейл разряда ебанутейших.
- **Dragon Age 2**. Упомянутая выше студия кройки и шитья «Электронные искусства» наебала доверчивых юзеров: сначала создатель игрушки BioWare (которого EA купила с потрохами) распустил слух о том, что SecuROM им не нужен. Однако по выходу игры выяснилось, что все совсем даже наоборот. Фаны игры ощутили прилив энергии счастья!
- **Final Fantasy VII** . Epic fail. В августе 2012, а-ля под конец света, вышла переизданная версия финал фантзи 7 и … сразу же зашла обратно. Причина немного банальна — судя по внутреннему строению потрохов онлайн-активации секурома, издателем был перепутан приватный RSA-ключ для дешифровки HWID, а юзвери всем детсадом отправлялись на йух.
- **paul.dll**. Он же *SecuROM PA (Product Activation)*. Некоторые антивирусы опознают данный файл как вирус и немедленно удаляют с компьютера анонимусов. В итоге, сабж отказывается запускаться. Алсо, вопреки устоявшемуся мнению, алгоритм проверки unlock кода находится в защищенном .exe файле, а паша.длл, всего навсего, играет роль конфетной обвертки, из которой можно почерпнуть только коды возврата для правильной/неправильной активации.
- **Sony DADC SecuROM version 8**. По большому счету по новой версии сабжа хэккер-коммунити набрало в рот ~~пива~~ воды и хранит молчание. Но эльфы уже намекают, что *8-я версия = упрощенная SecuROM 7.35*. No comments.

It's SecuROM

«Stop dumping VM's! Save the whales! »

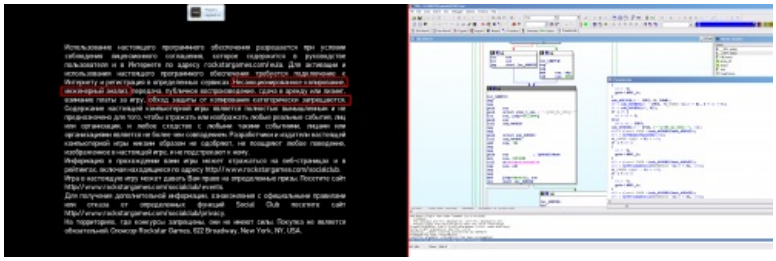
— В кряке для GTA IV от Razor 1911

Кроме интересных технических решений на прикладном уровне отдельным строем идут лулзы от разработчиков. ASCII-фраза **It's SecuROM** используется для идентификации и присутствует в специальном зашифрованном блоке данных. Для крекеров профит заключается в служебной информации о текущей версии сабжа и его фичах. Блок вшит в главный исполняемый файл и находится в PE-хидере.

Троллинг взломщиков

Первое, с чем сталкиваются наглые хэккеры, которые беспощадно пытаются переварить обратно машинный код разработчиков — философские фразы (**AND DWORD PTR DS:[EAX], EAX** машинный код, ♂☻символы♀☺), существующие в виде текстовых строк в ASCII-формате. По сути, бессмысленный набор букв и символов, но с особым смыслом:

- **< space for rent >** (правильный русский перевод: *рекламное место сдается*). До поры до времени самая канонічная фраза в сабже 7 версии. Впихивалась в самое начало виртуальной машины (VM) и откровенно доставляла.
По упорно ходящим слухам, два неизвестных науке крэкера на полном серьезе восприняли данный лулз и написали письмо в Sony DADC с просьбой купить рекламное место за круглую сумму и заменить надпись на *«Здесь были Вася и Петя! Пишите нам: Vasya@mail.ru, Petya@mail.ru»*. В Сони ДАДЦ, глубоко охуев от прочитанного, откровенно обиделись и в следующей версии фразу заменили на банальный «You Are Now In A Restricted Area».



Не поверите господа! Ломаю и плачу, ломаю и плачу…

К слову сказать, виртуальная машина сыграла с её разработчиками злую шутку: наличие VM было на руку взломщикам, так как через нее, как по проспекту, можно было попасть в OEP. Вследствие чего весь процесс получения дампа был проще, чем обоссать два пальца после полторашки Очаковского, что не могло не радовать всех хацкеров.
- **yates stilL Here kinda Ooooh** (правильный русский перевод: *Йейтс все еще тут, типа ооx*). Фраза также была задетекчена в VM. По дохлым слухам, Йейтс — то ли домашняя псина, то ли кот Рейгарда. Особы, приближенные к кругам разработчиков, утверждают, что Yates — это реальный человек, вполне себе толковый программист, вышедший из крекерской среды. Смысл троллинга заключался в присутствии возможности отодрать VM от игрушки, что является верхом мастерства взлома особо сложъный защит.
- **Виртуальная машина такая как есть**. Собственно, ее исполнение, само собой, вызывало немало лулзов. Вся дилемма в том, что любая VM по своей природе работает очень медленно. Из-за этого все разрабы машинок идут следующим проторенным путем:

    1. Запил общего каркаса VM
    2. Исправление своих ошибок

3. Добавление свистелок и переделок
4. Исправление своих ошибок
5. Добавление обфускации кода
6. Исправление своих ошибок
7. *«Бля-я-я-ть!!!! Игра стала грузиться очень до хуя времени, вместо 20 секунд. Сука! Ебаный насос! Надо заняться оптимизацией.»*[4]

И тут в последний момент начинается судорожный поиск, что требуется упростить и что нужно вообще выкинуть из виртуальной машины нахуй! В 7-м секуроме это выглядело так: существовало ровно 255 примитивов машинного кода VM, и все они должны были быть защищены обфускацией кода… Но старина Рейнгард схитрил и высадил на измену: чтобы виртуальная машинка работала быстрей, 2 самых ходовых примитива содержали совершенно открытый, «чистый» код, что невозбранно доставляло. Используя сей факт, можно было точно убедиться, как работает сие виртуальное чудо, и в конце концов выдрать его к австрийским ебеням из защищаемой программы, получив свеженький NoCD/NoDVD.

- † **MOV EAX, DEADC0DE** († *Сдохший код*). Без задорных извращений с машинным кодом тоже не обошлось. В 16-й системе счисления число 0xDEADC0DE выглядит как словосочетание на аглицкой мове **Dead Code**, что в переводе на русский буквально звучит как *сдохший код*. Цимес состоит в том, что остальной машинный код, который имеет отношение к данной инструкции, по сути также является мертвым мусором, то есть разработчики сабжа выступают здесь в роли великого Капитана Очевидности.
- **Magic Byte** . После первых вышедших билдов 7-й версии секурома на крекерских форумах некоторые, побывавшие внутри этого клондайка ассемблерных артефактов, стали нагнетать ощущение конца света и ужас, заявляя о том, что хекнуть защиту можно, подправив всего один магический байт. Сообщество тут же разделилось на три лагеря: первые говорили, что чокнулись сами крекеры, вторые высказывали мнение, что таки крыша поехала у сони дадц, третьим изначально было похуй. Доподлинно неизвестно, чем бы все закончилось, если бы разрабы дээрмэ не участвовали в срачах на крек-форумах, так как следующий билд SecuROM'a сразу снизил градус неадеквата по этому вопросу. Похоже, дыра таки была, но залатали.

Анекдот про улитку

Как оказалось, начиная с 8^{й} версии, теперь не обязательно использовать браузер, чтоб заходить на анедотсру. Целые анекдоты прямо в Вашем отладчике — инновация, хуле!
Самый известный про улитку в баре: 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?.)".
Очевидно, что с 9^{й} версии в секцию *.securom* обязательно введут аудиозаписи концертов Миши Задорнова.

Копиздинг кода у SafeDisc

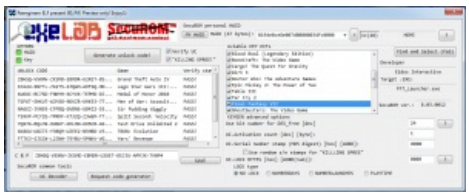
Не так давно выяснился еще один интересный парадокс — некоторые куски машинного кода Безопасного диска версии 4.x и SecuROM 7.3x похожи чуть более, чем полностью. Так как SafeDisc 4 вышел гораздо раньше (2005 г. от первого прихода) седьмой версии секурома (2007 г. от первого прихода), напрашивается вывод, что Sony DADC таки утянула исходный код. Правда, есть информация, что две конторы заключили внебрачный союз против союза StarForce-SolidShield[5].

Однако вполне резонно предположить, что все разрабы DeRьMa сами занимаются реверсингом продуктов своих конкурентов, дабы посмотреть, что нового те придумали, чтобы потом спиздить себе. Serious business is so serious!

Пиратский диск в приводе, как лицензионный

В начале марта 2013 гэ, появилась информация, что наши сцупермегокрэкеры учились…учились, ИЧСХ таки научились без Alcohol'ей, Daemon Tools'ов и вообще без оригинального диска патчить сабж так, чтоб он распознавал левые пиратские диски с базара в Мухосранске как настоящие лицензионные, что нелегально штампует Sony DADC AG! Запасаемся попкорном.

Кейген для онлайн-активации SecuROM PA



ДА! Еще один дичайший epic win: после взлома китайцами Denuvo, на сайте краклаба был анонсирован генератор unlock code. Онлайн-активация представляла из себя генерацию unlock code с помощью криптоалгоритмов **DES** (в трех вариантах) и **RSA** (последняя проверка HWID). Часть кода позаимствована с проекта OpenSSL. Request unlock code (код-запрос) содержал HWID и хэш заготовки индивидуального DES ключа игрушки. Сгенерированный unlock code представлял из себя две части — служебная структура и HWID.
Официальный сайт онлайн-активации секурома стал теперь не нужен.
К радости анонимусов, вышел наконец-то в паблик 17 января 2016 г. Накрыл напалмом сразу все игры,

защищенные SecuROM с требованием онлайн-активации. НА САМОМ ДЕЛЕ «напалмом» подобные игры накрывает одна чёткая библиотечка (2012 года рождения), которая, будучи кинутой в папку с борзой игрушкой, начисто предотвращает появление окна активации и, внимание, секуромовского запроса диска без каких-либо телодвижений с кейгеном. Анонимусом уже проверено на трёх тайтлах, и это только начало. Так-то.

BigFish games

В использовании технологии онлайн-активации SecuROM больше всех лоханулась пиндосская контора Big Fish, которая штапует PC-трэшак использую сраную технологию Adobe Flash. Янки купили SecuROM версии 8.03.12 с возможностью активации Trial-режима. Секуромовский Trial-mode немного отличается от традиционного способа активации, тем что сама активация производится строго через сервер. Однако-с, существует гениальный сплойт обламывания Trial-mode:

1. Заменяем текущую новую версию *paul.dll* (обычно v2.x) в каталоге игрушки на древнюю версию *paul.dll* (v 1.x)
2. Получаем возможность «Manual activation» (активация вручную)**!**
3. Юзаем 80_PA кейген
4. Сбрасываем в служебной структуре LOCK-биты
5. Генерируем свободный unlock code
6. Вставляем и активируем
7. ...
8. PROFIT!!!

Впрочем, опытные взломщики уже давно в курсе, что ввиду неразвитости этого Trial-режима, обойтись можно и без кейгена: контрольная функция в *paul.dll*, всего навсего, должна вернуть **1**(единицу). Естественно, добится этого можно банально использовав любой отладчик.
Окончательно топит секуромовский Trial-mode сказочная тупость самих разработчиков из BigFish: неучтенные особенности запуска приложений Adobe Flash! Парадокс, но главное приложение .exe любой выпущенной PC-игрушки представляло собой простую обвертку, которая, с помощью, нехитрой командной строки, запускала интерпретатор. Последний, естественно, не был защищен SecuROM! Стоило ли говорить, что, в данном случае, кряк к трэшевым PC-игрушкам от BigFish писался МАКСИМУМ за ДВЕ минуты.

Забавный факт: русскоязычный сайт BigFish предагает ТОЛЬКО игры для iPhone, iPad и iPod touch. PC-версий говноигрушек с секуромом там нет, что как бы намекает.

Коды ошибок и методы их обхода

Рейнгард предупреждае

Это должен знать каждый крякер.

Код ошибки (указан в скобках)	Что значит	Как обойти
1000	Выньте резервную копию диска	**Наебать** проверку геометрии диска секурома, запатчив 3 (три) раза код вида: • `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` (*(спойлер:* 0, 1, 1*)*)
2000	Дебаггер палится через PEB(*IsDebuggerPresent*)	Всегда сбрасывать флаг BeingDebugged
2001	GetTickCount возвращает всегда ноль	Суть схожа с кодом ошибки *8007*. Некоторые плаги или нубы, скрывающие отладчик, хукают функцию GetTickCount, заставляя ее возвращать всегда ноль (например, типичной банальной припиской **XOR EAX, EAX** в конце). Посему необходимо отключать данную фитчу и не трогать GetTickCount вообще, ибо сабж **не** юзает антиотладочные приемы, основанные на подсчете времени исполнения кода(RDTSC, GetTickCount и тд).
	Дебаггер палится через	Патчить код из SEH-обработчика на инструкциях UD2 *или*

3000	аппаратные точки останова(Hardware Breakpoints)	ставить аппаратки после проверки (модуль проверки аппараток идет 2 раза в начале и 2 раза после успешной проверки диска)
5000	Дебаггер/хакерская тузла(в 95% - Process Monitor) палится через *FindWindow*	Патчить *FindWindow* и возвращать всегда минус адын *или* менять название в главном окне твоей хакерской тузлы, которую разрабы уже занесли в черный список.
5001	Дебаггер(в 95% - SoftIce) палится через *CreateFile*	Патчить *CreateFile* и возвращать всегда минус адын *или* найти кулхакеское расширение для софтайса.
5002	Дебаггер/хакерская тузла(Process Monitor) палится через *FindWindowEx*	Патчить *FindWindowEx* и возвращать всегда минус адын *или* менять название в главном окне твоей хакерской тузлы, которую разрабы уже занесли в черный список.
6000	Программные точки останова в начале ВыньАПИ	Не надо ставить INT3 на первой/второй инструкции
6005	Аналогично 13001,с той лишь разницей, что для секции кода (после окончательной распаковки, перед прыжком на OEP) и другим алгоритмом(CRC32?).	Не надо ставить INT3 в проверяемых местах. Для остальных пряморуких-ставим аппаратную точку останова по чтению/записи на проверяемый участок, выскакиваем на алгоритме подсчета, и сразу после RET попадаем на условие срабатывания типа: • MOV ECX,DWORD PTR DS:[EDI+ECX+0x13A] • CMP EAX,ECX
8002	Дебаггер виден через *CheckRemoteDebuggerPresent* (шо в NTDLL)	Патчить CheckRemoteDebuggerPresent, возвращая ноль (поправь меня анон, если минус адын)
8007	Проверка на целостность *IsDebuggerPresent* не пройдена (возвращаемое контрольное значение изменено[6])	Будучи новичком в деле взлома, ты запатчил *IsDebuggerPresent* инструкцией **XOR EAX, EAX**(когда можно банально сбросить флаг BeingDebugged и не ебаться)
8011	Дебаггер палится по *ZwQueryInformationProcess* (шо в NTDLL), аргумент *ProcessInfoClass* = **7**	Запатчить *ZwQueryInformationProcess*. Вернуть любую хуиту, кроме нуля.
8019	Дебаггер палится по *ZwQueryInformationProcess* (шо в NTDLL), аргумент *ProcessInfoClass* = **31**(*0x1F*)	Запатчить *ZwQueryInformationProcess*. Вернуть любую хуиту, кроме нуля.
9000	Проебан файл **dfe** *или* **dfa**, которые используются для расшифровки данных в data файлах защищаемой игрушки. Во всем виноват SecuROM Дата файло активэйшен, сцуко.	Достать файлы с интернета
10000	Дебаггер палится по имени процесса-родителя.	Переименовать *ollydbg.exe* в *lurkmore.exe* и т. д. Данной поебенью, например, не страдает SND Olly.
13000	Нарушена целостность защищаемого .exe файла	SecuROM открывает сам себя(.exe файл)через WinAPI *CreateFile*, и методично считает контрольную сумму в секциях, считыавя байты *ReadFile*. Обломать это можно двумя способами: • Самый боянистый, который используют еще со времен StarForce 3.x, когда *protect.dll* надо было нафаршировать своим исполняемым кодом. Копируется оригинальный файл *filename.exe* и сразу переименовывается в какой нибудь *filename_original.exe*. В *filename.exe* вставляют перехватчик, который кидает хук на *CreateFile*(что в kernel32) и при попытке защиты открыть *filename.exe*, делает редирект на *filename_original.exe* • Чисто секуромовский. После *CloseHandle* открытого *filename.exe*, правится первая попавшаяся инструкция: ◦ `POPFD... CMP EAX, 1` (*(спойлер:* **0**-файл цел, все ок; **1**-файл поврежден; **2**-проверка не пройдена*)*)

13001	Нарушена целостность PE-заголовка файла	В подавляющем большинстве случаев, ошибка возникает при попытке добавить в таблицу импорта новые функции, например через LordPE™ или PeTools™. SecuROM имеет запасной оригинальный PE-хидер, который сравнивается через XOR с шагом, в 4 байта, с Вашим пропатченным: • `XOR ECX,DWORD PTR DS:[EDX]` • `NOT EAX` • `XOR ECX,EDX` • `CMP EAX,ECX` • `MOV EAX,EDX`
Целая строка: **Conflict with Emulation Software detected**	Кривое эмулирование торможения диска этим Вашим даемон тулсом. Фейл при сравнении скорости кругляшка.	Такая нездоровая херь характерна для многоядерных процессоров. Если не помогло ручное назначение одного ядра target-процессу в таскманагере, лечится в отладчике: Нужна найти *DeviceIoControl* с аргументом *IoControlCode* = IOCTRL_DISK_PERFOMANCE(0x70020). Обычно это отдельная функция находится цикле и заводится в новом потоке, при активной проверке геометрии. В конце цикла что-то типа: • `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]` Короче, *DeviceIoControl* должна возвратить в **EAX** ноль. Секуром понимает, что проверить скорость нельзя и пропускает модуль. Epic win!

Дисциплины

Вполне очевидно, что секуром является предметом срачей в специальных дисциплинах, по большей части устраиваемых жунализдами в своих статейках:

- **StarForce vs SecuROM** — что круче?
- **StarForce-SolidShield vs SecuROM-SafeDisc** — кто пидарасы, а кто д'Артаньян?

Особняком идут разборки между бандитскими группировками *SkidROW* и *RELOADED* с применением автоматов и гранатометов.

ООО «Секур»

Алсо, на просторах незалежної України есть фирма «Секур»[1], которая занимается (и что бы Вы подумали) импортом охранных побрекушек. Однако, анон не в курсе, контролируется ли она через офшоры Sony DADC или самим Рейнгардом.

Denuvo

Основная статья: ***Denuvo***

Печальный итог

Уже более 10 лет DRM-производители пытаются побороть пиратство в этой стране! И что же мы имеем на данный момент:

- Производство DRM — бизнес со своим блэкджеком и шлюхами.
- Пиратство уверенно растет с каждым годом.
- В большинстве случаев действует поговорка «Они бы сначала свой SecuROM защитили, потом бы эту GTA»
- Блаукович не стал спасателем мира от нелицензионных копий, а будущее его продукта весьма сумрачно.
- The Pirate Bay рулит!
- Россиянские власти активно заняты решением проблемы наряду с освоением нанотехнологий.
- на 7 месяцев перацтво таки побеждено. Крекеры куплены, секуром 9 (Denuvo) ломают не мэтры, а сопли зеленые, в час по чайной ложке. Второму уровню пищевой цепочки дали подзаработать на

активациях. Впрочем, учитывая тот факт, что на сей защите выходили игры далеко не то, что первого, даже второго сорта, всем, кроме школьников, насрать.

Галерея

Кошмарный сон Рейнгарда Блауковича

Сука!

ОН SHI--

Amazon.com проебал ключ

Кругооборот легального юзера в саппорте

Школьник, качаешь с PirateBay? Ты следующий!

Фейлы. Тысячи их!

Руткит, говорите?. Рейнгард скрывает!

Петросянство буржуйских журнализдов

Видео

Hitler rants about SecuROM
Гитлер и секуром

https://www.youtube.com/watch?v=p8A0cSSinAg
Fuck EA, fuck SecuROM

Тибериумный реверсинг. Продолжение
Лулзовое продолжение тибериумного реверсинга

Hitler rants about the PC version of GTA IV I
Гитлер и секуром в GTA IV

Тибериумный реверсинг
Тибериумный реверсинг

Тибериумный реверсинг. 80_PA SecuROM keygen. GTA IV, TRON Evolution, Bioshock, Final Fantasy ...
Тибериумный реверсинг. Кейген для онлайн-активации

Ссылки

- Посмотреть списокоту запротекченных игр и порадоваться за их разрабов (так как все уже давно взломано)
- Секуром ~~глючит~~ работает в GTAIV на раз, два, три, четыре...thousands them!
- Старые интересные новости о сабже (на языке королевы Елизаветы)
- **Законченные долбоёбы** из **Protection Technology** сами признаются, что **нарушают авторское право!** Разреверсили DRM CD-Cops от *LinkDataSecurity* и скопиздили алгоритм проверки диска оттуда. Крэкеры знают правду
- 80_PA последней версии 1.3.2 с over 100 крякнутыми играми

См. также

- DRM
- StarForce
- Таблэтка

Примечания

1. ↑ Хотя назвать DRM можно с натяжкой, ибо по всем характеристикам первое поколение однозначно сливало тройке SecuROM, SafeDisc, StarForce
2. ↑ Все открыто-диссасемблируй не хочу. У Рейнгарда с его секуромом челюсти бы отьехали от увиденного.
3. ↑ Основатель конторки CD Projekt Red, которая напилила игру
4. ↑ Исключение: старфорс. Его звезданутые разработчики, наоборот, только еще больше запихивают мусорного кода и засирают VM в космических масштабах, ибо они есть хронические долбоебы.
5. ↑ Подтверждением сего служит тот факт, что Sony и Macrovision ведут одинаковый «черный список» крекерского софта, который изрядно гадит их продуктам и портит им самим настроение.
6. ↑ Да!Да! Уважаемый Анон! Блаукович тоже читал книжки Криса Касперски и в курсе, что *IsDebuggerPresent* банально считывает значение флага *BeingDebugged* из структуры PEB. Соответственно SecuROM сначала просто вызывает данную функцию, а потом ВНЕЗАПНО как возьмет и сам положит в *BeingDebugged* свою циферку от балды и проверяет появилась ли она на выходе *IsDebuggerPresent*

Игры

1C 3dfx A challenger appears Action 52 Aion Alignment All your base are belong to us Angry Birds Angry Video Game Nerd Another World Arcanum Assassin's Creed Baldur's Gate Barrens chat BASKA Battletoads Beat 'em up BioWare Bitches and whores Blizzard Blood Brick Game Bridget Carmageddon Chris-chan Civilization Combats.ru Command & Conquer Company of Heroes 2 Contra Copyright Corovaneer Online Counter-Strike Crimsonland Crysis Daggerfall Dance Dance Revolution Dangerous Dave Dark Souls Dead Space Demonophobia Denuvo Deus Ex Diablo Did he drop any good loot? Digger Disciples Doki Doki Literature Club! Doom DOOM: Repercussions of Evil Dopefish DotA Dreamcast Duke Nukem 3D Dune 2 Dungeon Keeper Dungeons and Dragons Dwarf Fortress Earthworm Jim Elasto Mania Elite EVE Online Everquest 2 F-19 Falcon Punch Fallout Fate/stay night Five Nights at Freddy's Flashback FPS GAME OVER Game.exe GameDev.ru GamerSuper Garry's Mod Giant Enemy Crab GoHa.Ru Gothic Granado Espada Grand Theft Auto Guilty Gear Guitar Hero Half-Life Half-life.ru Heroes of Might and Magic Hit-and-run Hitman HL Boom Homeworld I.M. Meen Ice-Pick Lodge IDDQD Immolate Improved! It's dangerous to go alone! Take this. Itpedia Jagged Alliance Kantai Collection Katawa Shoujo Kerbal Space Program Killer Instinct

Пиратство

1C Copyright Denuvo Direct Connect DRM EDonkey2000 GamerSuper I2P Infostore Metallica Microsoft Neogame Nintendo NoNaMe One Piece P2P Rapidshare RGHost Rutracker.org SecuROM SOPA StarForce Steam The Pirate Bay Акелла Варез Горбушка Денис Попов Дискета Диски с приколами Единый реестр запрещённых сайтов Зайцев.нет Компьютерные пираты Копираст Списрач Крякер инета Кулхацкер Либрусек Линукс Литрес Морские пираты Никита Михалков Нойзбункер Пиратские игры девяностых Радиопираты Распечатать лицензию на Линукс Российское авторское общество Русефекации Русский щит Сомалийские пираты Таблэтка ТНТ Файлообменник Фаргус Хакер Экранка Яблочник

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype StarForce Steam T9 Tor Vi Windows Windows 7 Windows Phone 7 Windows Phone 8

Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман Машинный перевод Мегапиксель

Deutschland über alles!

14/88 Adidas Angry German Kid Bf.109 Crysis Die Ärzte Int Jedem das Seine Junkers Ju 87 Kraftwerk Mp3 NichtLustig Rammstein Rapidshare SAP SecuROM Waffen-SS X macht frei Z0r.de Аненербе Бальдур фон Ширах Берлинская стена Бомбардировка Дрездена Бумер Вагнер Ван дер Люббе Великая Отечественная война Вундервафля Газенваген ГДР Геббельс Гелендваген Герман Геринг Германия Гитлер Гламурный фашизм Гунтер фон Хагенс Екатерина II Заговор генералов И если один скажет «зиг»… Йозеф Менгеле Когда они пришли… Лейбниц Леннарт Поттеринг Магнитофон Макс Раабе Метрополис Мнение Гитлера Мюнхенский сговор Национал-гомосексуалисты Ницше Окончательное решение Онкель Ханс Пакт Молотова-Риббентропа Панцерфауст Первая мировая война Протекторат Богемии и Моравии Свастика Сумрачный гений Танк «Тигр» Тахарруш Тим Кречмер Токио Готель Тоталитарное искусство Трабант Уве Болл Унгерн Унтерменш Фошыст Шушпангевер Шушпанцер Эрнст Рём