

Denuvo — Lurkmore



НЕНАВИСТЬ!

Данный текст содержит зашкаливающее количество НЕНАВИСТИ. Мы настоятельно рекомендуем убрать от мониторов людей, животных со слабой психикой, кормящих женщин и детей.

Denuvo (англ. *Denuvo Anti-Tamper*, рус. *Денуво, Дануево, Дерънуво*) — очередное творение копирастов в области весёлой, **бессмысленной и беспощадной** защиты **интеллектуальных прав**, преемник ранее отпизженного SecuROMa. Несмотря на озвученную цель, **DeРьМом** сабж ВНЕЗАПНО не является (см. [ниже](#)).

Немного истории

После того, как **SecuROM** эпично разломали в TP, Sony DADC AG таки выгнала мудаков-разработчиков [на мороз](#). Двое из них — Рейнгард Блаукович и Роберт Эрнандес быстро нашли себе хату на другом конце города Зальцбурга, сделали на оставшиеся деньги там евроремонт и родили на свет новую защиту — **Denuvo**. ИЧСХ, эту самую Денуву начали позиционировать не как DRM, а как [en.w:Anti-Tamper Software](#). Впрочем, все однозначно сошлись во мнении: как говно ни назови, быть говном оно не перестанет. Желаящие опробовать сию НЁХ в своих высерах нашлись достаточно быстро: **FIFA 15**, **Lords of the Fallen** и, чуть позже, **Dragon Age: Inquisition**. Причём в лучших секуромовских традициях, все защищённые этой хренью игры люто, бешено глючили и лагали даже на топовых компах. Но не это стало самой главной новостью! Норот, который уже выстроился в очереди на ведущих торрент-трекерах, ожидал **кряка** к этим трем играм, а его всё не было и не было. Данной ситуацией умело воспользовались разработчики сабжа, чтобы повыпендриваться и потроллить пиратов, мол, **«смотрите, какая у нас, блядь, непробиваемая защита!»**. Говн в вентилятор решили подбросить и **игрожуры** с заголовками типа «Защита, которая убивает ваш SSD», «Непробиваемая Denuvo», **«Ubisoft платит хакерам за взлом Denuvo»**... Тысячи их! Все это рождало **тонны срачей** на [форумах](#) и в [комментах](#).

Время шло, а кряки так и не спешили появляться. При таком раскладе дерънува действительно могла оказаться «крутой защитой»®... Но в конце концов, молитвы были услышаны — китайская хакерская группа 3DM выкатила сообщение на своей страничке, что Denuvo они всё-таки сломали, но им нужно время, чтобы проверить работу кряков. С этого момента игрожуры и игросайты начали поливать жидким говном теперь уже разработчиков Denuvo, мол, «допизделись». Впрочем, радость длилась не долго. В январе 2016 китайцы из группы 3DM, обломавшие зубы о гранит науки Just Cause 3 громко заявили, что денува **наносит ответный удар** улучшается не по дням, а по часам, и с такими темпами через 2 года **торрент-идишона не видать**, запустив очередную волну слухов о её непробиваемости.

Скандалы, интриги

Denuvo.com

Самым первым лулзом, который приключился с только что рожденным брендом, породил официальный сайт сабжевой конторки. Дело в том, что тот проработал буквально день-два и... отправился в **астрал**, где и просушился почти месяц. Настоящая причина анону не известна, но версий без пруфов конспирологи нарожали порядочно:

- сайт [denuvo.com](#) **взломали пираты** после того, как прошла новость о новой защите (делать им больше нечего);
- сайт [denuvo.com](#) коллективно **задудосили** геймеры после того, как **узнали**, что в новую **GTA V** собираются встроить этот трэш, который к тому же ещё и **НИВЗЛАМАТЬ!!1**;
- сайт [denuvo.com](#) упал сам по себе из-за **говнокодинга** (тоже высокая вероятность, кодить-то что сайт, что дерьмо требует рук);
- **админ** сайта [denuvo.com](#) на следующие утро после корпоратива just for lulz сделал из под рута **rm -rf /***, как и в случае, когда рухнули сервера онлайн-активации SecuROM PA после выхода Bioshock.



Лого разработ



Наконец-то что-то написали про то, как это говно взламывается



Denuvo всепоглощающая

История повторяется.

Забагованность защиты

С учётом всего вышесказанного неудивительно, что после выхода Денувы бурной рекой потекли жалобы на кучу багов и вылетов игрушек по вине этого анти-тампера. Жалобщиков можно условно поделить на три группы:

1. **Счастливые покупатели лицензионных копий™**, которые начали высирать **кирпичи** по поводу багов и вылетов игрушек на форумах.
2. **Сами разработчики Lords of Fallen**, которые признали, что «Denuvo — забагованное дерьмо» (пруф просран).
3. Взломщики на том же краклабе.

VMProtect

В очередном кряке 3DM, на этот раз для Mad Max, **кто-то догадался** тулзой ProtectionID проверить файл 3dmgame.dll. И что бы вы думали — там используется VMProtect, только с хуя бы ему взяться в кряке от денувы?

Тут и всплыло: Denuvo оказался банально перекрашенным VMProtect. Это стало очевидным, после сравнения виртуальных машин обоих продуктов и по наличию зашифрованной dispatch-table. Во всех играх начиная с Lords of the Fallen и до Just Cause 3 использовалась VMProtect 2.0 (2.x). Кроме копирования виртуальной машины, Denuvo полностью копирует у VMProtect обфускацию кода. Учитывая, что этот самый дерьмопротект кулхацкеры выносят на раз-два, денува могла быть запросто попячена. Но, начиная с Just Cause 3, Блаукович понял, что скоро будет тибериумный реверсинг два, если не начать что-то менять в своём высере. В итоге выкинули dispatch-table из виртуальной машины, переместив delta-смещения в ленту p-code, соответственно тем самым, мы имеем перед собой уже современный VMProtect 3.x., а в таком виде он уже не настолько прост во взломе. Но взлом вполне возможен.

Стоит, кстати, отметить **Assassin's Creed: Syndicate** — он использует как раз таки настоящий VMProtect. А почему не Denuvo, он же ведь непробиваемый?! Очевидно, что в Ubisoft знали хитрый план Блауковича (или просто задушила жаба) и решили не переплачивать за нашумевший бренд. Конечно же, от «взлома за пару минут» это его не спасло — 3DM и CODEX за пару дней удалили защиту **к такой-то прабабушке**.

В пользу версии сдирания VMProtect есть ещё один не очевидный, но **железный** факт: все существующие **патенты Рейнгарда Блауковича** касаются на данный момент исключительно технологии проверки компакт-дисков. Если разработчики денувки брызгают слюной «защита абсолютно новая и не имеющая аналогов в мире»®, тогда получается парадокс, ибо любой дебил догадался бы сначала запатентовать новую технологию защиты, а потом штамповать её, спустя некоторое время. Объяснить данную нестыковку можно как раз тупым переклеиванием бирок и разводом лохов.

Ни для кого не секрет, что **StarForce** изначально своровала технологию защиты у CD-Cops. Есть объективное мнение, что и VMProtect Software поступили так же — архитектура построения виртуальной машины невозбранно спищена с **SolidShield 2**. Таким образом, это доказывает, что за последние несколько лет ничего принципиально нового разработчиками придумано не было.

История получила бурное развитие после публикации **этого поста** на краклабе. Оказывается, **авторы вмпрота** спустя ТРИ года решили устроить судебное разбирательство по данному вопросу.

3DM

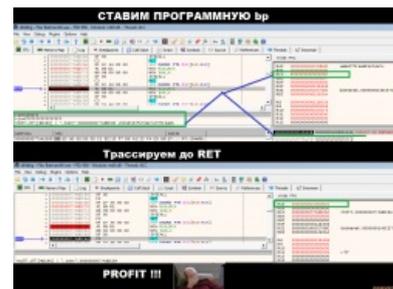
3DM — группа кулхацкеров, упомянутых выше, специализирующихся на взломе игорь. Китаёзы-горлопаны с бложиком и штатной тян. Лулзы генерят как специально. То они говорят, что почти поломали денуву (и это справедливо для ранних версий), то, блядь, что защита не взламываемая, мы в отпуск, а нищebroдам через 2 года ваще нипаиграть будет. Хомячки разделились на несколько лагерей: **те, которые говорят, что 3DM сдулись, колотят тех, кто говорит, что 3DM подкупили**.

Baldman

Суровый Российский **Кулхацкер**, один из первых полноценно взломал Denuvo v4, тем самым доказав, что на любую хитрую ДРМ найдётся свой кряк. Ушёл от дел также быстро, как и пришёл.

CONSPIR4CY

Никому доселе неизвестный итальянский клан крякеров, который ВНЕЗАПНО стала Мессией мира взлома денувы. До сих пор ни одна группа не смогла достичь такого огромного успеха в разрыве жопы



DENUVO: Мы знаем толк в проектировании анти-отладки! Расшифровка для задротов: защита видит программную точку останова на первой инструкции, корректно отработывает противодействие с инкрементом регистра... и даже не догадывается, что это её же антиотладочный трюк. Facepalm!

Блауковича, как CPU. Из наиболее значимых успехов - первые полноценные проперы на первые игры с деновой, взлом Resident Evil 7 за жалкие пять дней и анальный фистинг ушных Ubisoft и их гибридов Denuvo + VMProtect. Останавливаться не собираются, в отличие от сдувшихся китайцев.

STEAMPUNKS

Новый клан, в нашем пиратском море. Пошли ещё дальше и намутили генератор лицензий для Denuvo, тем самым ещё более унизив разработчиков. ИЧСХ, свои генераторы покрывают тем же VMProtect. Примечательны также тем, что взломали FIFA 18 и Total War: Warhammer 2 в день их выхода, доставив немало дискомфорта Бла-бла-блауковичу. Вместе со своими собутыльниками - крякерами из CODEX на время организовали альянс под именем CODEPUNKS, за время действия которого успели взломать South Park: The Fractured but Whole. Увы, после этого от стимпанков больше ничего не слышно.

REVOLT

Ещё одна группа хейтеров деновы, состоящая из одного единственного Voksi. Примечателен тем, что дорабатывает чужие кряки, давая возможность поиграть в мультиплеер на пиратке, обновляет игры к последним патчам и длц. Voksi был арестован болгарской полицией по заявке Irdeto - пиратил и не скрывался, надеясь, что ему не засунут паяльник в задницу в итоге

Skidrow

А вот и старички подъехали. Запилили кряк на последнюю версию Deus Ex на 02.03.17. тем самым начали огромные споры на форумах о том спёрли они кряк у CPU или запилили свой, а мы продолжаем сидеть с попкорном и наблюдать за этой драмой. Оказалось что эти «крякеры» просто взяли экзешник из Deus Ex Breach и запили в Mankind Divided, запустили до главного меню и отправили на торренты, не поняв что их высер работает криво. Несмотря на такой громкий провал, летом 2017 года посмели огрызнуться на CPU и STEAMPUNKS, назвав их кряки ненастоящими проперами, за что успешно обосраны остальной сценой и пиратами.

Denuvo.com leak

Несмотря на мифическую крутость™ denuvo в файлах различных говноигрушек, сайт деновы оказался эталонным [костылём](#) в электронной безопасности, а [5 февраля 2017 г. просторы интернета узнали](#):

1. что denuvo.com's admin is [lamer](#);
2. гораздо более важное — в сеть утекло [огромное](#) количество приватной информации;
3. матюги юзеров, адресованных Рейнгарду Блауковичу (reinhard.blaukovich@denuvo.com);
4. пароли, адреса, явки, контакты представителей серьезных контор с Блауковичем;
5. другая разная инфа.

Из <https://denuvo.com//download> были стянуты архивы *Denuvo_Introdection.zip* и *Insider_prot.zip* (весил 444 Мегайбата). Как выяснилось, всё оба были защищены, ВНЕЗАПНО, [SecuROMом](#). Ожидаемо через день на краклабе выкатили [специальный билд кейгена 80_PA](#).

Мифы и домыслы

- **DENUVO — новая DRM.** На самом деле Денува DRM НЕ является. Лицензия защиты распространяется только на противодействие отладчику и сокрытие исходного кода от реверс-инжиниринга (антидамп, обфускация, виртуальная машина). Денува не умеет проверять диски, проводить онлайн-активацию, и даже не имеет своего графического интерфейса, как когда-то всё это было в SecuROM. Что не помешало CPU убрать простенький Steam Stub, наложенный поверх Denuvo, из исполняемого файла Batman: Arkham Knight. От необходимости этот самый Denuvo эмулировать в steam_api64.dll удаление стимовского DRM отнюдь не избавило. Фактически, он выполняет функцию защиты от копирования, а конечному пользователю по барабану, как его называют сами разработчики.
- **DENUVO — это преемник StarForce.** Феерический бред, никакого отношения гейропейская *Denuvo Software Solutions GmbH* и русская *Protection Technology* друг к другу не имеют. Как уже неоднократно написано выше, защита использует часть технологий SecuROM, так что прямая линия идёт только к Sony DADC AG (что, в принципе, неудивительно). Единственное, что достойно упоминания: косвенное отношение к созданию DENUVO может иметь [TagesSAS](#)^[1].
- **DENUVO портит SSD.** Исчерпывающих данных с развернутыми ассемблерными листингами шифрования и дешифрования файлов во время работы никто до сих пор не приводил. Доподлинно доказан только факт медленной работы [защищенного приложения](#) из-за обилия обфускации, вызовов виртуальной машины, плохой оптимизации, пожирания памяти выделенными страницами в 4096 байт, а также загаживания [OEP](#). Всё это усугубляется особенностями платформы x64 (в отличие от x86) — более высокие требования к CPU (в частности, необходимость большого объёма внутреннего кэша) ради обеспечения достаточной скорости декодирования веток^[2].
- **Denuvo не снижает производительность в играх** — относительно свежий вброс от [PR-менеджеров](#) «Денуво ГмбХ», нацеленный на полоумных дебилов и [детешек](#). На деле фраза представляет собой

никакой ценности и представляют собой несколько часов унылого геймплея с последующим удалением. Зачем нужна защита для игры, которую всё равно надо купить для онлайн, ведь серверы только лицензионные? **А разгадка одна:** жадность. Поэтому даже новая часть Need for Speed будет с защитой, не говоря уже про новый **Mass Effect**, Titanfall, и никому не вравшуюся FIFA. Из крупных издателей, которые не побрезговали замарать руки во имя профита, отметились также **Square Enix** с известными сериями **Hitman** и **Deus Ex**. Если обмазывание **Сорокльсыго** можно объяснить неуверенностью в коммерческом успехе игры, потому что Absolution как-то неприятно порвала шаблон всем, то аугментирование дерьмом Адама Дженсена не понятно — ведь Human Revolution, несмотря на очевидные недостатки, очень полюбилась публике, и все неравнодушные гарантировали бы успех новой игре. А разгадка одна — новая часть оказалась **сладким хлебушкой**, да еще и с микротранзакциями. Внезапно, не побрезговала обмазаться **несвежим** даже **Ubisoft**, которая в последнее время выпускала и выпускает не менее несвежие поделия, и которая презирала Денуво вместе с Глаукашом — даже сиквел **высера** Watch Dogs обзавёлся этой **инновацией**. К празднику жизни подключился и Тодд Говард со своей **Bethesda Softworks** после феерических обосрамсов с **Fallout 4**, когда защиту, к ёбаному стыду, сломали *за неделю до релиза*, и попыткой продавать моды на **Скайрим** за деньги. Впрочем, в последующем их политика изменилась — Rage 2 вышла в Bethesda.net с дополнительным исполняемым файлом без Denuvo, а через некоторое время этот форк стал основным, **Doom Eternal** в версии для Bethesda.net также получил такой дополнительный экзешник (на радость пиратам, взломавшим игру всего за 3-4 часа). Из новых пациентов SEGA с **Dawn of War III** и даже **Sonic Mania**, которая фактически является закосом под классику.



Сравнение продаж игр одной серии. Демотивирует разработчиков игр

Когда итальянцам из CPU удалось выдать полноценный крик для Лары, не требующий свистоплясок со **Стимом**, казалось, что до масштабного взлома всех новейших проектов ещё далеко, но всё случилось гораздо быстрее. И таки на **Голиафа** нашёлся **Давид**. Сегодня все утверждения о том, что Денуво совершенно непобедима, оказались brutally втоптаны в говно, что и показывают взломы — если раньше взломанная игра была целым событием, то теперь стало всё как раньше и **новинку** можно найти на торрентах в кратчайшие сроки после релиза. Глаукомич с компанией всего лишь тянули время, и теперь каждое обновление защиты **только раззадоривает** взломщиков. Поскольку **непобедимая защита™** теперь стала бесполезной тратой денег, с ноября 2016 года шоу стали покидать его главные участники, упомянутые выше — DOOM, Hitman, Titanfall и Mass Effect: Andromeda.

22 января 2018 года CPU в очередной раз насрала на Denuvo, взломав версию 4.8 [1]. В ответ на это Denuvo в кратчайшие сроки **из подручных материалов** склеила версию 5.0, которую уже успели впилить в файтинг Marvel vs. Capcom: Infinite. Ноябрь 2018 года отметился тем, что появилась новая группа хацкеров FCKDRM. Вместе с CPU и CODEX они яростно атаковали дерьнуво, в результате на торрентах опазались такие игры, как Final Fantasy 15 и Far Cry 5 со всеми вышедшими обновлениями и DLC, Shadow of the Tomb Raider, Assassin's Creed: Odyssey и похождения лысого со штрихкодом 2 аж за несколько дней до релиза.

Irdeto покупает жопу Блауковича

В начале 2018 г., в Амстердаме состоялась стрела по поводу покупки жоп разработчиков DENUVO некими нидерландскими говнокодерами [2]. Традиционно, наш краклуб идёт впереди планеты — аналитика развития событий была представлена следующая:

Так что ждите, гибридов (помимо того, что там уже будет Steam-Origin-Uplay):

1. Cloakware Cybersecurity + DENUVO
2. Cloakware Cybersecurity + DENUVO + VMProtect
3. Cloakware Cybersecurity + DENUVO + VMProtect + (что-то ещё)

Впервые было применено новое слово **гибриды**. Судя по всему, эльф хотел сказать, что разработчики решили заняться скрещиванием нескольких типов защит или совместить несколько защит в одном файле. Что из этого выйдет — покажет время.

Видео

Тибериумный реверсинг. In a pursuit of DENUVO cracking

Тибериумный реверсинг про DENUVO. Как ни странно, но непосредственно взлома Unravel там нет, зато полностью обыграна тема «VMProtect в DENUVO»

Примечания

- [↑](#) Журнал «Хакер» #199. [Заметка про DENUVO в секуромовской статье.](#)
- [↑](#) Длина инструкций выросла! В некоторых случаях более, чем в два раза. Также исчезла условная адресация, которая была в x86-режиме. Подробно обо всех этих прелестях можно прочитать в книге Криса Касперски «Искусство дизассемблирования», в которой отладке программ на x64 посвящена целая глава. Бесплатно, к примеру [тут](#).

См. также

- [Варез](#)
- [Таблэтка](#)
- [Neogame](#)



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 Кописрач 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 Вarez 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