Игра ата мега

Ата игра мега

Посмотрите это видео от разработчиков Atomega, чтобы лучше разобраться с геймплеем игры и понять её сильные стороны.

Иногда Google Play может удалять некоторые приложения, поскольку они не соответствуют их требованиям. Кроме того, они могут быть недоступными для скачивания в определённых странах. В таком случае единственный способ получить данное приложение - это скачать его APK-файл:

Если у вас возникнут дополнительные вопросы, всегда будет рады Вам помочь.

Сентябрь ознаменовался сразу двумя крупными взломами, от которых пострадали компании Uber и Rockstar Games. Очень похоже, что за этими атаками стоял один и тот же подросток.

Мега ата игра

Первой от компрометации пострадала компания Uber, и злоумышленник охотно поделился со СМИ скриншотами внутренних систем жертвы. Судя по ним, он получил полный доступ ко многим критически важным системам Uber, включая защитное ПО компании и домен Windows.

Также взломщик добрался до консоли Amazon Web Services, виртуальных машин VMware vSphere/ESXi, панели администратора электронной почты Google Workspace и сервера Slack, на котором публиковал сообщения, и bug bounty программы компании на HackerOne.

Журналистам нескольких изданий удалось пообщаться с хакером, и тот похвастался, что ему всего 18 лет и он взломал Uber, используя социальную инженерию, так как «у компании слабая безопасность».

Самое интересное: ответственность за эту атаку в Uber возложили на участника хак-группы Lapsus$, о которой мы писали не раз. Напомню, что весной 2022 года после череды громких атак на Nvidia, Samsung, Microsoft и Okta полиция Лондона арестовала семь человек в возрасте от 16 лет до 21 года «в связи с расследованием деятельности хакерской группы».

Ата мега игра

В настоящее время все они находятся под следствием, а двум подросткам предъявлены обвинения. Эти аресты совпали с объявлением о том, что несколько членов Lapsus$ на время уходят в отпуск, и с тех пор активность группы практически сошла на нет.

Но похоже, в Uber считают, что правоохранительные органы нашли далеко не всех участников Lapsus$.

Вскоре после Uber атаке подверглась компания Rockstar Games, что привело к одной из крупнейших утечек в истории игровой индустрии. В результате этого взлома в сеть попали десятки роликов с геймплеем еще не вышедшей GTA VI (их слил сам хакер), и взломщик заявил, что украл «исходный код и ассеты GTA V и VI, а также тестовую сборку GTA VI».

При этом злоумышленник, скрывающийся под никами teapots2022 и teapotuberhacker, утверждает, что именно он скомпрометировал Uber немногим ранее. Teapotuberhacker писал, что не ожидал такого внимания и даже хотел «договориться» с Rockstar Games и Take-Two Interactive (издатель и владелец компании Rockstar Games), судя по всему — желая потребовать у компаний деньги.

Мега ата игра

Однако масштабы этих инцидентов быстро привлекли к случившемуся внимание властей и правоохранительных органов, и уже несколько дней спустя полиция лондонского Сити сообщила об аресте 17-летнего подростка из Оксфордшира. Его обвиняют в двух случаях нарушения условий освобождения под залог, а также в двух компьютерных преступлениях. Его имя не раскрывается, так как он несовершеннолетний.

После этого многие ИБ-эксперты и известный журналист Мэтью Киз (со ссылкой на собственные источники) писали, что именно задержанный стоял за недавними громкими взломами компаний Uber и Rockstar Games. При этом Мэтью Киз и его источники подтверждают: арестованный подросток — это участник Lapsus$, которого ранее уже арестовывали за взлом Microsoft и Nvidia.

Известно, что задержанный своей вины пока не признал и остается под стражей.

Согласно статистике компании Google, количество уникальных доменов верхнего уровня, ссылки на которые требуют удалить правообладатели (в соответствии с законом США «Об авторском праве в цифровую эпоху», DMCA), в этом месяце перевалило за 4 000 000.

Игра мега ата

В общей сложности за всю «историю наблюдений» у Google требовали удаления 6 миллиардов URL. С такими требованиями к компании за прошедшие годы обращался 326 221 правообладатель.

Больше всего запросов, 579,5 миллиона, поступило от BPI LTD — British Phonographic Industry, ассоциации, в которую входят Universal Music UK, Sony Music UK и Warner Music UK.

ИБ-специалисты сообщили, что билдер известного шифровальщика LockBit опубликован в открытом доступе. Судя по всему, LockBit 3.0 слил в сеть недовольный разработчик или конкурент одноименной группировки.

Напомню, что хак-группа LockBit выпустила обновленную малварь LockBit версии 3.0 в июне 2022 года и вместе с этим представила собственную вымогательскую программу bug bounty, предлагая другим злоумышленникам деньги за интересные уязвимости.

Мега ата игра

Как теперь сообщил ИБ-исследователь, известный под ником 3xp0rt, недавно зарегистрированный пользователь Twitter по имени Ali Qushji утверждает, что вместе с командой он взломал серверы LockBit и обнаружил там билдер шифровальщика LockBit 3.0, который и поспешил слить в открытый доступ.

После этого другой известный ИБ-эксперт vx-underground подтвердил, что еще 10 сентября с ними связался пользователь с ником protonleaks и тоже поделился копией того же билдера. При этом, по словам vx-underground, официальный представитель группировки LockBit утверждает, что никакого взлома вообще не было, а приватный билдер распространяет недовольный руководством хак-группы наемный разработчик.

ИБ-специалисты уверены, что вне зависимости от источника этой утечки публикация билдера LockBit 3.0 в сети, скорее всего, увеличит количество вымогательских атак. Ведь билдер позволяет преступникам быстро создавать исполняемые файлы, необходимые для запуска собственной кампании (включая сам шифровальщик, дешифровщик и специализированные инструменты).

По сути, инструмент состоит из четырех файлов: генератора ключей шифрования, самого билдера, изменяемого файла конфигурации и batch-файла для сборки всех файлов. Так, файл config.json можно использовать для настройки шифровальщика, в том числе отредактировать записку с требованием выкупа, изменить параметры конфигурации, перечислить, какие процессы и службы следует завершить, и даже задать управляющий сервер, куда малварь будет отправлять данные. То есть ничто не мешает любым злоумышленникам связать вредонос со своей собственной инфраструктурой.

Ата игра мега

К сожалению, прогнозы экспертов начинают сбываться. Утекший билдер уже взяла на вооружение хак-группа Bl00Dy, построив с его помощью шифровальщик, который затем использовался для атаки на неназванную украинскую компанию.

Летом 2022 года исследователи Group-IB зафиксировали двукратный рост количества выложенных в открытый доступ баз данных российских компаний (по сравнению с весной этого года).

За три летних месяца в сеть попало 140 баз, причем антирекорд был поставлен в августе — 100 утечек. Общее количество строк всех летних сливов равняется примерно 304 миллионам.

Этот антирекорд эксперты связывают с «мегаутечкой», которая включала базы данных сразу 75 российских компаний. Для сравнения: за всю весну текущего года было опубликовано всего 73 базы.

Мега игра ата

Самые крупные утечки были зафиксированы у компаний, работающих в сферах доставки — 192 миллиона строк, онлайн-видео — 43 миллиона строк, медицинских услуг — 30 миллионов строк.

Mozilla сообщает, что кнопки обратной связи на YouTube практически не работают. Даже если пользователь ясно дает понять, что ему что-то не нравится, подобные рекомендации все равно продолжают поступать.

Чтобы собрать данные, связанные с реальными видео и пользователями, исследователи Mozilla привлекли к исследованию добровольцев, которые применяли браузерное расширение RegretsReporter. Оно накладывает на YouTube-ролики, которые просматривают пользователи, общую кнопку «Прекратить рекомендовать». При этом на бэкенде пользователей зачисляют в случайную группу, и каждый раз, когда они нажимают эту общую кнопку, на YouTube отправляются разные сигналы: «Не нравится», «Не интересует», «Не рекомендовать этот канал», «Удалить из истории». Также из пользователей образуется контрольная группа, от которой на YouTube не поступает никакой обратной связи.

Используя данные, собранные из 500 миллионов рекомендованных видео, исследователи создали более 44 тысяч пар видео — одно «отклоненное» видео и видео, впоследствии рекомендованное YouTube. Затем исследователи оценивали эти пары или использовали машинное обучение, чтобы решить, была ли рекомендация похожа на видео, которое ранее уже отклонил пользователь.

Игра мега ата

Как показало сравнение с контрольной группой, отправка сигналов «Не нравится» и «Не интересует» практически неэффективна и не предотвращает нежелательные рекомендации от YouTube (было предотвращено лишь 12% из 11% нежелательных рекомендаций). Кнопки «Не рекомендовать канал» и «Удалить из истории» оказались чуть более эффективными — они предотвратили 43% и 29% нежелательных рекомендаций. Однако исследователи подчеркивают, что инструментов, которые предлагает YouTube, недостаточно, чтобы избавиться от нежелательного контента.

«YouTube должен уважать отзывы пользователей, рассматривая их как значимые сигналы о том, как люди хотят проводить свое время на платформе», — пишут исследователи.

Представитель YouTube Елена Эрнандес (Elena Hernandez) объясняет, что такое поведение платформы преднамеренно, поскольку YouTube вовсе не пытается отсекать весь контент, связанный с какой-либо темой. При этом Эрнандес раскритиковала отчет Mozilla, заявив, что в нем не учитывается, как устроены элементы управления YouTube.

«Важно, что наши элементы управления не отфильтровывают целые темы или точки зрения, так как это может иметь негативные последствия для зрителей, создавая „эхо-камеры“, — говорит Эрнандес. — Мы приветствуем академические исследования на нашей платформе, поэтому недавно мы расширили доступ к Data API через исследовательскую программу YouTube. Но в отчете Mozilla не учитывается, как на самом деле работают наши системы».

Мега ата игра

По ее словам, определение «похожего», которое использует Mozilla, не принимает во внимание, как устроена система рекомендаций на YouTube. По словам Эрнандес, функция «Неинтересно» удаляет конкретное видео, а кнопка «Не рекомендовать этот канал» предотвращает рекомендации с конкретного канала в будущем. Она объясняет, что в таких случаях YouTube вовсе не стремится вообще прекратить рекомендации любого контента, связанного с конкретной темой, мнением или спикером.

На Восточном экономическом форуме зампред правления Сбербанк Станислав Кузнецов рассказал, что с начала третьего квартала 2022 года банк отразил свыше 450 DDoS-атак, а это больше, чем за последние 5 лет суммарно.При этом атакам подвергается не только сам банк, но и его пользователи. Так, к основным видам нарушений на сегодняшний день можно отнести фишинг и телефонное мошенничество, и с ними в Сбербанке борются, в том числе при помощи библиотеки с голосами преступников.

«Важно, как мы противостоим [атакам], какими личными разработками мы пользуемся. Одной из них является использование библиотеки голосов преступников, библиотеки голосов мошенников. И именно эта библиотека нам сегодня помогает продвинуться достаточно уверенно вперед по противодействию телефонному мошенничеству. Мы для себя обнаружили следующий тренд. Видимо, мошенники каким-то образом понимают, что они уже становятся на контроль, и они уходят из „Сбера“. То есть эти преступники, голоса которых записаны в нашей библиотеке, фактически уходят из „Сбера“ и от клиентов „Сбера“ и таргетируют свои усилия на клиентах других кредитных организаций»,

— рассказал Кузнецов, добавив, что в настоящее время библиотека насчитывает примерно тысячу голосов.

Игра ата мега

Разработчики «хакерского тамагочи» Flipper Zero рассказали, что уже два месяца не могут вернуть 1,3 миллиона долларов, которые остались на заблокированном без указания причин PayPal-аккаунте проекта. Что происходит, не может объяснить даже поддержка PayPal, и разработчики говорят, что производство Flipper Zero под угрозой.

Напомню, что в 2020 году на Kickstarter собрали рекордные 4 882 784 доллара на производство «хакерского тамагочи» и крайне интересного мультитула Flipper Zero, о создании которого мы тогда поговорили с одним из его авторов Павлом Жовнером.

В начале 2022 года участники Kickstarter-кампании стали получать свои гаджеты, а в июне наконец стартовала открытая продажа Flipper Zero. Вскоре после этого бизнес-аккаунт PayPal заблокировали, о чем разработчики сообщили в официальном Twitter проекта.

Команда Flipper Zero рассказывает, что около половины покупателей выбрали PayPal в качестве способа оплаты (также заказ можно было оплатить банковской картой напрямую), но уже через несколько дней PayPal инициировал проверку аккаунта. «Они попросили какие-то [дополнительные] документы, и мы сразу их предоставили», — пишет команда.

Игра ата мега

За этим последовало еще несколько запросов от PayPal, на которые разработчики так же ответили, но в итоге они получили лишь сообщение о перманентном бане бизнес-аккаунта Flipper Zero.

«Мы обращались в поддержку PayPal, но даже они не могут сказать, чего именно от нас хочет комплаенс-команда. Сейчас нам нужно платить за новые партии продукции, и эти деньги имеют решающее значение для нашего бизнеса. Если кто-то из нашего сообщества имеет прямые контакты внутренней команды PayPal и может как-то повлиять на ситуацию, мы просим вашей помощи», — гласит официальное обращение создателей Flipper Zero.

Эксперты Qrator Labs уже в седьмой раз изучили влияние возможных сбоев сетей системообразующих операторов связи на глобальную доступность национальных сегментов интернета. Выяснилось, что в 2022 году Россия потеряла сразу 8 позиций, сместившись на 10-е место в топ-20.

Если в 2016 году для попадания в топ-20 достаточно было иметь процент потенциального отказа сетей чуть более 8%, то сейчас даже показателя в 6,5% уже недостаточно, чтобы оказаться в лидерах.

Игра ата мега

В мире явно прослеживается тенденция повышения отказоустойчивости: средний показатель надежности улучшился с 35,84% до 26,7%.

Рейтинг отказоустойчивости интернета в целом достаточно стабильный показатель развития связи уже много лет подряд, и в 2022 году в нем произошло сразу несколько значительных изменений. Ключевые таковы:

В России процент потенциального отказа сетей непрерывно возрастает уже в течение 4 лет. По мнению аналитиков, это точно связано с продолжающимися процессами как организационной, так и технической консолидации отрасли. Поэтому вероятность того, что в 2023 году Россия тоже покинет топ-20, довольно высока.

При этом в России находится шестая из крупнейших в мире точек обмена трафиком — MSK-IX, охватывающая 7 городов-миллионников. Как пишут эксперты, это еще раз подтверждает, что РФ не использует имеющийся у нее колоссальный потенциал по связности в полной мере.

Игра ата мега

В сентябре произошло событие, в реальность которого было бы сложно поверить еще пару лет назад: на сайте Nullsoft опубликовали финальную версию Winamp 5.9, которая теперь доступна всем желающим.

За долгие годы своего существования Winamp проделал сложный путь и не раз переходил от одной компании к другой. Так, компанию Nullsoft, создавшую Winamp, еще в 1999 году приобрела AOL, которая и поддерживала плеер на протяжении многих лет. Затем в 2013 году разработку программы, уже растерявшей немалую долю своей популярности, решили прекратить, сайт Winamp.com закрылся (последней версией стала 5.666), а права на Winamp в 2014 году выкупила бельгийская компания Radionomy, занимающаяся интернет-радиовещанием.

С тех пор никаких новостей о медиаплеере почти не поступало. Лишь осенью 2018 года представители Radionomy неожиданно сообщили, что в 2019 году Winamp преобразится, станет лучше и вернется в строй. Разработчики заявляли, что намерены сделать Winamp универсальным решением для прослушивания всего — подкастов, радио, плейлистов и так далее.

Кроме того, в сентябре 2018 года пользователи обнаружили в сети утекшую бета-версию Winamp 5.8, где были исправлены некоторые баги и появилась поддержка Microsoft Audio. Тогда было не совсем ясно, откуда взялась новая версия и кто стоял за ее разработкой. Но вскоре глава Radionomy Александр Сабунджан (Alexandre Saboundjian) прояснил, что над Winamp 5.8 работала именно Radionomy. Новая версия содержит исправления для различных багов, в том числе касающихся совместимости с Windows 10, а также убирает из медиаплеера все платные функции, внедренные в Winamp раньше.

Мега игра ата

К сожалению, обещанного релиза обновленного Winamp в 2019 году пользователи так и не дождались, а версия Winamp 5.8 на протяжении четырех лет так и оставалась самой новой. Тем не менее в конце прошлого года сайт Winamp.com неожиданно претерпел кардинальный редизайн и на нем появился новый логотип медиаплеера. Также на сайте стало можно зарегистрироваться для участия в бета-тестировании нового Winamp, которое обещали начать совсем скоро.

Теперь бета-тест наконец окончен и Winamp 5.9 Final Build 9999 представили широкой публике.

«Это кульминация труда двух команд разработчиков, длившегося четыре года (с момента выпуска 5.8) и прерывавшегося из-за пандемии, — пишет команда в примечаниях к релизу. — Конечному пользователю может показаться, что изменений не так много, но самой большой и сложной частью стал перенос всего проекта с VS2008 на VS2019 и его успешная сборка».

Действительно, самым заметным изменением в Winamp 5.9 стал перенос приложения из Visual Studio 2008 в Visual Studio 2019. Причем этот перенос спровоцировал множество проблем с плагинами в более ранних версиях плеера среди пользователей, у которых не был установлен Visual Studio 2019 Redistributable. В финальном релизе установщик Winamp сам проверит, все ли нужные файлы Visual Studio 2019 есть, и при необходимости предложит установить их.

Мега ата игра

Также в журнале изменений сообщается, что в этом релизе улучшена поддержка Windows 11, потоковое вещание через HTTPS://, добавлен новый каталог подкастов и поддержка воспроизведения в высоком разрешении, улучшена поддержка .itz, .mdz, .s3z и .xmz, а поддержка юникода теперь работает нормально.

Хотя в Winamp 5.9 устранили множество ошибок, разработчики обещают, что в версии 5.9.1 будет исправлено еще больше известных багов. Среди них: ошибки в диалоговом окне «О программе», Milkdrop, редакторе AVS, подкастах ml_wire, скине Bento.

Есть и не слишком хорошие новости для тех, кому нужен декодер NSV VP3, — эта функция теперь признана устаревшей.

«Мы нигде не можем найти старый исходный код On2 VP3, поэтому официально объявляем этот формат устаревшим», — поясняют разработчики.

Ата игра мега

Скачать обновленный Winamp 5.9 можно на официальном сайте Nullsoft.

Журналисты Business Insider решили выяснить, сколько зарабатывают специалисты Google на разных должностях. Для этого они изучили заявления на получение рабочей визы H-1B, где необходимо указывать предполагаемый базовый оклад. В составленный в итоге список вошли зарплаты в офисах Google в Калифорнии, Вашингтоне и Нью-Йорке. Зарплаты приведены за год.

Аналитики из компании Mandiant предупредили о появлении троянизированной версии утилиты PuTTY, предположительно созданной северокорейскими хакерами из группы UNC4034 (она же Temp.Hermit или Labyrinth Chollima). Судя по всему, вредоносная версия PuTTY используется, чтобы взламывать организации, которые представляют интерес для злоумышленников.

Обычно такие атаки начинаются с того, что злоумышленники связываются со своими целями по электронной почте и делают им заманчивое предложение, якобы приглашая их на работу в Amazon. Затем хакеры отправляют жертве сообщение в WhatsApp, в котором делятся файлом amazon_assessment.iso. В последнее время файлы ISO все чаще используются для заражения машин под управлением Windows, потому что двойной клик по ним по умолчанию приводит к их монтированию.

Игра ата мега

ISO включает в себя текстовый файл (readme.txt), содержащий IP-адрес и учетные данные для входа, а также вредоносную версию PuTTY (PuTTY.exe). Интересно, что хакеры также используют в своих атаках SSH-клиент KiTTY (форк PuTTY), в таких случаях имя файла будет Amazon-KiTTY.exe.

Пока неясно, как именно строится диалог между злоумышленниками и жертвами, но, похоже, хакеры убеждали жертв открыть ISO-образ и использовать предложенный SSH-инструмент и учетные данные для подключения к хосту, чтобы пройти некое тестирование.

Хотя вредоносная версия PuTTY оснащалась вредоносной полезной нагрузкой, она была полностью функциональной (так как скомпилирована из легитимной версии программы). Но исследователи обращают внимание на то, что легитимные версии PuTTY подписаны разработчиком, а версии хакеров — нет.

Отчет Mandiant гласит, что хакеры модифицировали функцию connect_to_host() таким образом, чтобы при успешном SSH-подключении с использованием приложенных учетных данных развертывался вредоносный шелл-код DAVESHELL в формате библиотеки DLL (colorui.dll), упакованной с Themida.

Мега ата игра

Чтобы сделать запуск шелл-кода незаметным, вредоносная PuTTY использует уязвимость в colorcpl.exe, а DAVESHELL действует как дроппер финального пейлоада — бэкдора AIRDRY.V2, который выполняется непосредственно в памяти.

По данным исследователей, по сравнению с предыдущей версией AIRDRY новый вариант поддерживает меньше команд, зато добавлены новые возможности: выполнение в памяти и обновление ключа AES для связи с управляющим сервером.

На фоне ухода из России крупных киностудий и иностранных стриминговых сервисов в Рунете заметно выросло количество ссылок с пиратским контентом. Чаще всего пираты выкладывают голливудские премьеры, однако, по словам участников рынка, сложнее защищать становится и российские сериалы, кино и шоу.

В Яндексе сообщают, что летом заблокировали на 42% больше ссылок (9,1 миллиона за июнь — август против 6,4 миллиона прошлым летом), а в «Газпром-медиа» говорят о росте блокировок на 25% (до 1,64 миллиона) во втором квартале.

Мега ата игра

Хакер, известный под псевдонимом CTurt, давно специализируется на взломе игровых консолей. Теперь он продемонстрировал свежий PoC-эксплоит Mast1c0re, который называет «практически неустранимой» дырой в безопасности PS4 и PS5. Mast1c0re должен позволить устанавливать и запускать на консолях Sony произвольные приложения.

CTurt рассказывает, что продемонстрировал Mast1c0re представителям Sony еще год назад, через программу bug bounty, но так и не дождался выхода публичного исправления.

В своей работе Mast1c0re полагается на ошибки JIT-компиляции, которую использует эмулятор, запускающий определенные игры для PS2 на консолях PS4 и PS5. Эта компиляция дает эмулятору специальные разрешения на непрерывную запись PS4-ready-кода (на основе оригинальных исходников для PS2) непосредственно перед тем, как этот код будет выполнен на уровне приложений (application layer). Получив контроль над обеими сторонами этого процесса, хакер может написать привилегированный код, который система в итоге сочтет легитимным и безопасным.

«Поскольку мы используем системные вызовы JIT по прямому назначению, на самом деле это даже не эксплоит, а просто хитрый трюк», — комментирует CTurt.

Ата мега игра

Исследователь пишет, что получить контроль над эмулятором теоретически позволяют любые известные эксплоиты, которые давным-давно существуют для PS2-игр. Хотя некоторые из них можно активировать буквально одним нажатием кнопки, для большинства потребуется использовать некую известную игру и доступ к специально отформатированному файлу сохранения на карте памяти, что приведет к переполнению буфера и откроет доступ к защищенной памяти. Нужно отметить, что похожие эксплоиты использовались для взлома PSP и Nintendo 3DS на протяжении многих лет.

К сожалению, этот способ немного ограничен из-за того, что PS4 и PS5 не могут распознать стандартные диски для PS2. Это означает, что любая эксплуатируемая игра должна быть доступна в виде загружаемой через PSN игры PS2-на-PS4 либо это должна быть одна из тех немногих игр для PS2, что выходили на физических дисках, совместимых с PS4.

Получить готовый для эксплуатации файл сохранения PS2 на PS4 тоже не так просто. CTurt рассказывает, что ему пришлось использовать уже взломанную PS4 для цифровой подписи модифицированного файла сохранения игры Okage Shadow King, чтобы тот работал с его PSN ID. Затем CTurt с помощью системной функции импорта сохранений на USB загрузил файл в целевую систему.

Подготовив этот «фундамент», CTurt наконец перешел к сложной серии переполнений буфера и стека, утечек памяти и эксплоитам для RAM, которые он использовал для получения контроля над эмулятором PS2. В итоге он сумел получить доступ к встроенным функциям загрузчика для передачи ISO-файла PS2 по локальной сети, а затем дать эмулятору команду загрузить эту игру через виртуальный диск.

Ата игра мега

Однако загрузка других игр для PS2 в эмулятор — это хорошо, но настоящей целью CTurt было воспользоваться этой точкой входа, чтобы запускать произвольный код в системе. Этот процесс хакер обещает детально описать в следующей статье, как и повышение привилегий, которое необходимо для запуска любого кода «в контексте игр для PS4».

По сути, хакерам по-прежнему придется использовать отдельный (и потенциально поддающийся исправлению) эксплоит ядра, чтобы получить «полный контроль» над PS4, объясняет CTurt. Но Mast1c0re уже должно быть достаточно для запуска сложных программ, «включая JIT-оптимизированные эмуляторы и, вероятно, даже некоторые пиратские коммерческие игры для PS4».

Также, по словам CTurt, Mast1c0re теоретически может послужить точкой входа для компрометации гипервизора PS5, который

управляет низкоуровневой системной безопасностью на этой консоли.

CTurt подчеркивает, что закрыть дыру, которую использует Mast1c0re, практически невозможно. Дело в том, что эксплуатируемый эмулятор PS2 упакован с каждой доступной игрой PS2-на-PS4, а не хранится отдельно, как часть операционной системы консоли.

Ата мега игра

То есть для физических дисков PS2-на-PS4 эксплоит будет работать, пока пользователь отказывается от онлайн-обновлений перед игрой. А для цифровых релизов это означает, что, даже если эксплоит исправлен, существуют методы перейти на сохраненную версию, пригодную для эксплуатации, с использованием проксированного HTTP-трафика с локального сервера.

«Проблема неисправима не с технической точки зрения, но в том смысле, что так устроена консоль и они не будут ее менять. Если у вас есть эксплуатируемая игра (цифровая или физическая), Sony будет сложно удалить или исправить ее на вашей консоли», — объясняет CTurt.

В похожей ситуации компания Nintendo приняла решение удалить эксплуатируемые 3DS-игры из Nintendo eShop, пытаясь ограничить возможный ущерб. Пока Sony не поступила так же с эксплуатируемыми играми для PS2 в PSN.