Misc

Misc development

3D-принтер, реверсинг, два экрана

Кто вайб-кодит – налетай. Кто сам пишет – убегай...

Некоторое время назад заинтересовался я 3D-печатью. Но вместо того, чтобы взять, как все нормальные люди, какой-нибудь Bambu Lab P1S, я взял QIDI Q2. Зачем? Конечно, чтобы ~~печатать TPU с использованием AMS~~ тратить свое время на решение всевозможных возникающих проблем. Эта статья как раз об одной из таких проблем.

А в чем, собственно, проблема? Как вы, наверное, знаете (или сейчас узнаете), многие 3D-принтеры имеют небольшой экран на корпусе, который позволяет им управлять (помимо управления через веб-интерфейс или, например, через мобильное приложение). Ниже можно увидеть, как внешне выглядит QIDI Q2 и обратить внимание на экран в его верхней части.

Так вот. После приобретения, длительной распаковки, снятия всяких там заглушек и фиксаторов и подключения системы AMS, я обнаружил, что подключенный тачскрин не подает признаков

жизни (экран не загорается, USB-порт на нем не функционирует).

Читать далее

Kaimi / 22 апреля, 2026 / C/C++, Python, Reversing / 3D, 3d-printer, linux, printer, qidi, qidi-q2, touchscreen / 2 комментария

EXE → MTX за секунды: JS-экстрактор для MyTestXPro

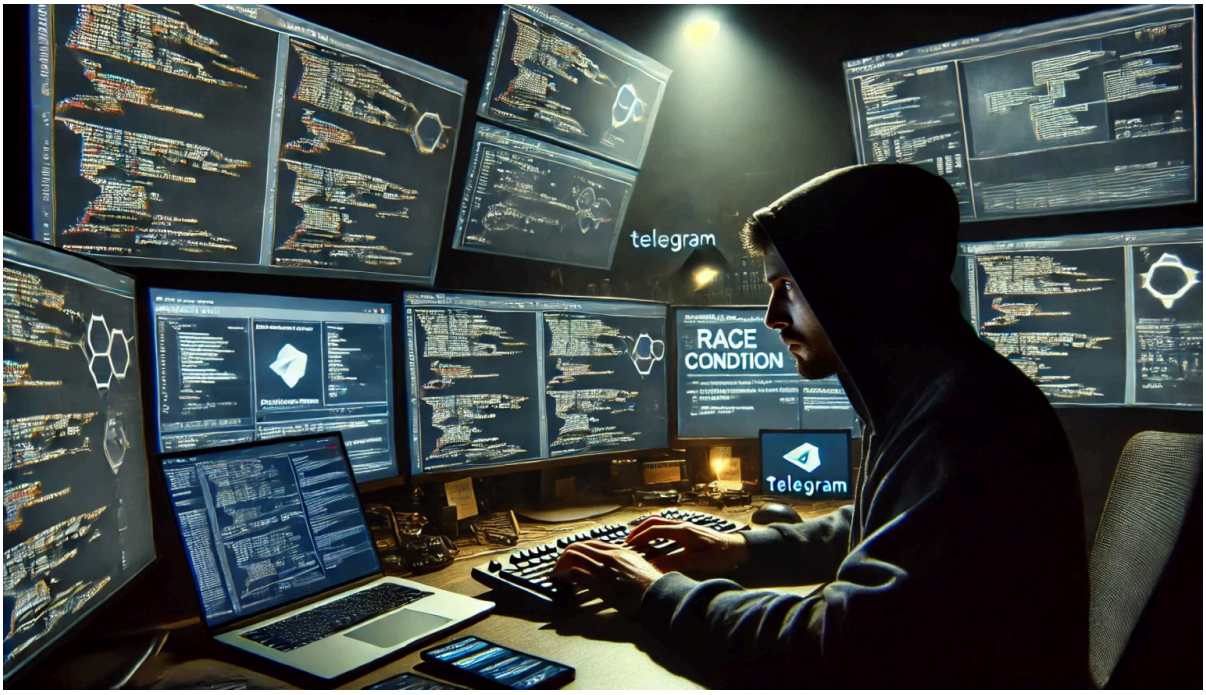
Разбирать MyTestX и MyTestXPro когда-то было целым квестом: нужен был отладчик (OllyDbg или x64dbg), виртуальная машина с Windows XP, утилита MyTestXProHelper и немного терпения... Все чтобы достать заветный .mtx из .exe-файла с тестом. Сегодня всё это превращается в "открыл страничку в браузере - указал файл - получил тест": новый клиент-сайд HTML/JS-скрипт без бэкенда делает всю работу прямо в вашем браузере.

Читать далее

Kaimi / 2 июля, 2025 / HTML/JS, Для новичков / mtx, MyTestX, mytestxpro / Добавить комментарий

Эксплуатация состояния гонки в «тапалках» в Telegram

За последние полгода-год в Telegram появилось множество так называемых мини-приложений, которые выдают некие фантики за совершённые действия, и обещают дать возможность конвертировать эти фантики в некоторые рыночные криптовалютные токены, которые можно будет продать за реальные деньги. В качестве примера можно привести: Hamster Kombat, Blum, CalmMe, CryptoRank, Flare X, StarChime... тысячи их. Конечно, максимальную потенциальную прибыль в таких активностях будут иметь люди, которые обладают выходом на большие аудитории и могут по реферальной ссылке завлечь людей в приложение, а также ботоводы с автокликлерами. Что же делать простым людям, которые хотят выжать что-то сверх доступных активностей в этих приложениях? Очевидно, искать уязвимости! Сегодня я приведу несколько примеров весьма тривиальных уязвимостей, которые позволяют немного накрутить баланс во многих "тапалках".



Читать далее

Kaimi / 8 августа, 2024 / Pentest, Для новичков / blum, calmme, crypto, mini apps, race condition, telegram, состояние гонки / 4 комментария

Вы многое упускаете в своих пентестах!

Перед началом пентеста ресурсов компании (будь это веб-сервисы или десктопное/мобильное приложение), часто приходится проводить предварительную разведку. Заказчик может специально не сообщать о конкретных эндпоинтах, которые требуется протестировать, поэтому их список (как и список дочерних доменов, функций приложения, параметров запросов, и т.д.) приходится собирать. Ведь от этого напрямую зависит, сколько уязвимостей и ошибок вы сможете найти. Если кто-то из участников теста смог найти эндпоинты, о которых другие тестеры ничего не знают, то шанс раскрыть в них ранее необнаруженные проблемы становится максимальным. А значит, и прибыль тоже увеличивается.

Найти скрытые параметры API, эндпоинты, и функции приложений возможно, обладая некоторыми знаниями о том, как работают средние и крупные бизнесы, и учитывая это при тестировании. Итак, что же нужно знать, и как достичь максимального покрытия при пентесте?

Читать далее

dx / 7 августа, 2024 / Pentest / coverage, experiments, holdouts, regional rollout / 2 комментария

Выигрываем в гоночки необычными способами

Всем привет, это **dx** (нет, это не Kaimi притворяется, это настоящий dx)! Сегодня мы поговорим об одном из частых программных багов, который регулярно приводит к уязвимостям, - гонках. Я не эксперт в их эксплуатации (в отличие от Kaimi, который, может быть, когда-нибудь поделится с вами хорошими примерами из своего опыта, а также современными методами и инструментами). Я же поделюсь знаниями с другой стороны баррикады, и расскажу, что такое гонки с точки зрения ПО, и какие факторы могут помочь "выиграть" при их эксплуатации.

Читать далее

dx / 3 августа, 2024 / Pentest / consensus, data race, race condition, TOCTOU / Добавить комментарий

Анализируем вызовы XFS API

Привет, дорогие мои скучающие по публикациям на блоге! Я знаю, что вы все ждали гениальных постов последние два года. Но, что я, что d_x заняты делами, которые по важности, честно сказать, уступают только спасению мира... или нет. Сегодняшняя тема - CEN/XFS, специфичный и крайне нужный стандарт для взаимодействия с банковским оборудованием, а конкретнее - способ анализа вызовов XFS API на Windows. Если вы до сих пор не знаете, что такое CEN/XFS

(не путать с XFS, который файловая система), то, скорее всего, у вас была счастливая жизнь без головной боли. Но для тех, кто готов погрузиться в это болото - welcome.

Читать далее

Kaimi / 25 июля, 2024 / Windows, Для новичков, ИБ, Сниппеты / winapi, windows, xfs, xml, сплайсинг / Добавить комментарий

20 лет проблем приема платежей

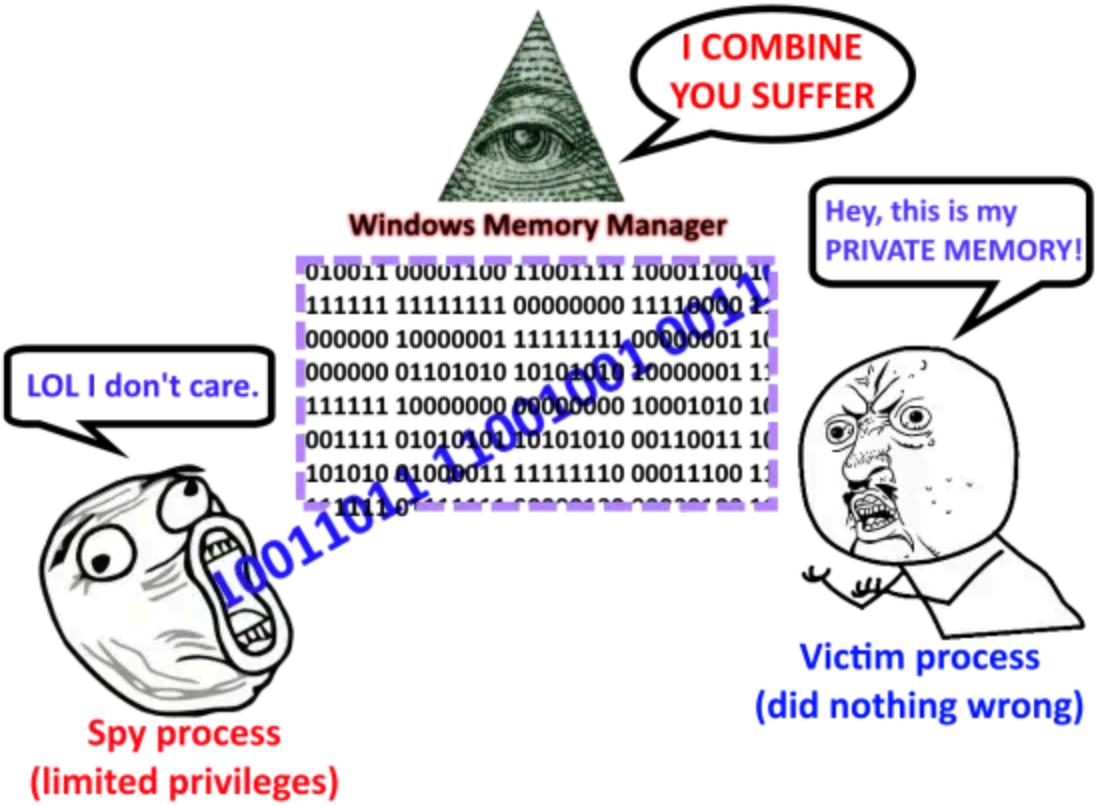
За логотип спасибо @yarbabin

Электронные системы расчетов существуют в интернете уже давно, а баги на них встречаются двадцатилетней давности. Мы находили критические уязвимости, позволяющие угнать деньги и накрутить баланс. Сегодня мы разберем типовые реализации приема платежей и связанные с ними проблемы безопасности.

Читать далее

Kaimi / 13 июля, 2022 / Pentest, Для новичков, Это интересно / payment systems, paypal, qiwi, race condition, webmoney, yoomoney, агрегация платежей, платежные системы, состояние гонки, уязвимости / 2 комментария

Чтение памяти чужого процесса через комбинирование памяти в Windows 10



Сразу скажу, что всё не так страшно, как звучит, и вы не сможете взять и прочитать память абсолютно любого взятого процесса в системе. По крайней мере, без некоторых предусловий. Основная уязвимость уже практически полностью прикрыта. Поэтому пост скорее предлагается в качестве исторической справки и для общего развития. Плюс, исходя из информации, которой я располагаю, никто пока не описывал такой способ эксплуатации, который предложу я.

Начну с того, что в Microsoft были уведомлены об этой проблеме ещё года полтора назад. В ответ мне сообщили, что уязвимость *в большей степени* уже закрыта, и что я могу опубликовать свои исследования.

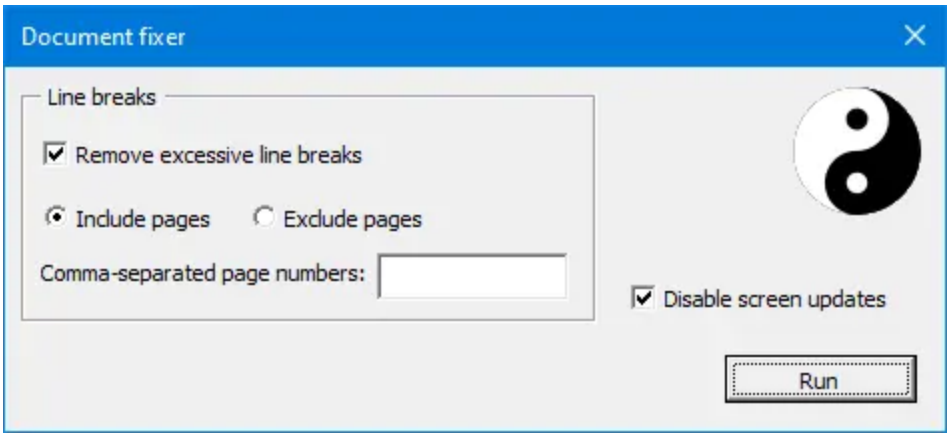
Итак, приступим. В Windows 8.1 и в Windows 10 в какой-то момент времени появилась такая фича, как комбинирование памяти (memory combining или page combining, хорошо описана в книге Windows Internals, 7 издание, 1 часть). Суть её достаточно проста: операционная система раз в 15 минут ищет в физической памяти страницы с одинаковым содержимым и объединяет их

в одну с целью экономии оперативной памяти. Те процессы, которые владели одинаковыми страницами, получают ссылки на новую общую страницу с атрибутом "только для чтения" и "копирования при записи" (read-only и copy-on-write). Если какой-то из процессов изменяет свою страницу, система при возникновении соответствующего copy-on-write исключения её копирует и снова размещает в физической памяти, а процесс снова получает индивидуальную копию этой страницы.

Читать далее

dx / 5 июля, 2020 / C/C++, Windows / Enable-MMAgent, Memory combining, page combining / 4 комментария

Пишем макросы для Microsoft Word с GUI like a PRO [Часть 2, финал]



Да, это макрос для MS Word!

Продолжаем тему макросов в Microsoft Word. Будем доделывать пользовательский интерфейс для нашего макроса замены двух и более последовательных переводов строки на единственный. Зачем вообще может понадобиться какой-то интерфейс для макроса? Ну, например, мы хотим удалить лишние переводы строки на всех страницах документа, кроме каких-то конкретных. Интерфейс позволил бы указать номера страниц документа, которые нужно при обработке

пропустить (либо наоборот, обработать только указанные страницы). Вот этот функционал и будем реализовывать.

Читать далее

dx / 28 июня, 2020 / Windows, Сниппеты / Macros, Microsoft Word, Word / Добавить комментарий

Пишем простой модуль для Acunetix

Некоторое время назад в сканере уязвимостей веб-приложений Acunetix появилась возможность расширения функционала за счет добавления собственных модулей. На официальном блоге даже была опубликована заметка, описывающая общий подход к разработке модулей. Давайте напишем простой модуль на основе нее, а также моей прошлогодней заметки по созданию модуля для Nessus. С точки зрения функций модуль будет аналогичным: поиск на узле скрипта Adminer, старые версии которого позволяют читать произвольные файлы на сервере с помощью фичи MySQL LOAD DATA LOCAL INFILE.

Читать далее

 Kaimi / 27 июня, 2020 / HTML/JS, Pentest, Для новичков / acunetix, adminer, автоматизация задач / 4 комментария

Misc / Сайт работает на WordPress