k i b e r t e s t . t e c h

Небезопасные пароли.
Сервис поиска

rudenko.dmitry@kibertest.tech
ООО "КИБЕРТЕСТ"
Руденко Дмитрий

Реестр МинЦифры #19353

7 . 9 2 7 . 5 3 1 . 7 2 . 3 6

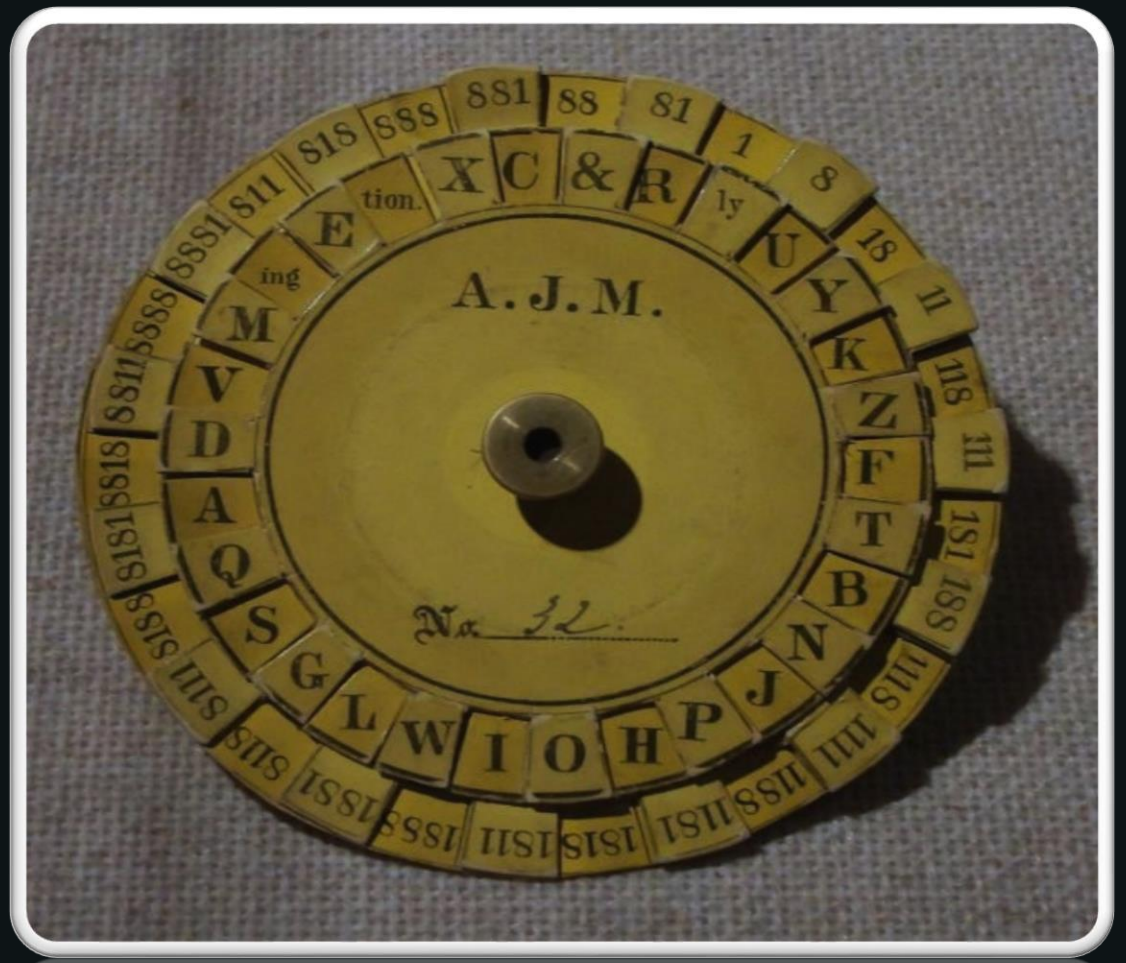
Государственная регистрация #2023614426

КЛЮЧЕВОЙ БИЗНЕС-РИСК

02

ПАРОЛИ...

..как ключи от дверей. Если вор их подберет - последствия непредсказуемы. Иногда (например, если взломали пароль клиента - пользователя сервиса) инцидент может приобрести огласку, что ведет к репутационным издержкам и оттоку клиентов. А ещё хакер может украсть базу клиентов, ноу-хау, удалить данные и т.д. Это - простои, нарушение бизнес-процессов.
ЗА ВЗЛОМОМ И УТЕЧКОЙ ПАРОЛЕЙ ПОЧТИ ВСЕГДА СЛЕДУЮТ "НЕПРИЯТНЫЕ ИЗДЕРЖКИ.



О ПРОДУКТЕ

Нет аналогов!

Российское решение, реализует локальный поиск потенциально опасных паролей в Вашей системе по предустановленной базе реально использовавшихся и утекших аутентификаторов

23+ млрд.

паролей в поставляемой базе

Слабые пароли есть всегда!

в среднем, обнаруживаем от 7 до 24% слабых паролей в контуре компании!

РЕШАЕМ ПРОБЛЕМЫ

СОТРУДНИК ЗАДАЛ СЛАБЫЙ ПАРОЛЬ. Перед сменой пароля он за 5 сек. проверит новый по базе из 23 млрд. утекших паролей

ПАРОЛЬ ВСКРЫТ ПЕРЕБОРОМ. Проверка учетных записей, выявление утекших паролей и оперативная замена на сильные пароли

ИСПОЛЬЗУЮТСЯ ТИПОВЫЕ ЛОГИНЫ. В этом случае критически важно, чтобы пароль был стойким к перебору по словарям, комбинациям и bruteforce

ОБХОД 2FA, RECAPTCHA, ограничение попыток ввода пароля и др. сервисы безопасности можно обойти. Вся надежда - на действительно сильный пароль

РЕШАЕМ ПРОБЛЕМЫ

05

HAVEIBEENPWNED НЕ ДАСТ ПРОВЕРИТЬ МНОГО ПАРОЛЕЙ. Вводить вручную сотни паролей нереально и небезопасно, т.к. админ получит доступ к паролям

"ЗАБЫТЫЕ" УЧЕТНЫЕ ЗАПИСИ. Сотрудник уволен, учетка осталась. Пароль не меняется. Возможность подбора пароля за неограниченное количество времени

СЛАБЫЙ АЛГОРИТМ ГЕНЕРАЦИИ ХЕШЕЙ Позволит хакеру быстро подобрать пароль, войти и закрепиться в системе, развивая дальнейшие векторы атак

ПУСТЫЕ И СТАРТОВЫЕ ПАРОЛИ. При сбросе / создании учетки часто ставится стартовый пароль. Если его не поменять, эту учетную запись может взломать хакер

Быстрое внедрение

Как правило, требуется не более 8 часов до перво-начального запуска

ПРЕИМУЩЕСТВА

06

База паролей

- встроена (23 млрд. строк)
- регулярно пополняется
- оптимизированная, универсальная

Расчёт HASH

- с использованием CPU
- с использованием GPU
- алгоритмы под разные ОС и системы

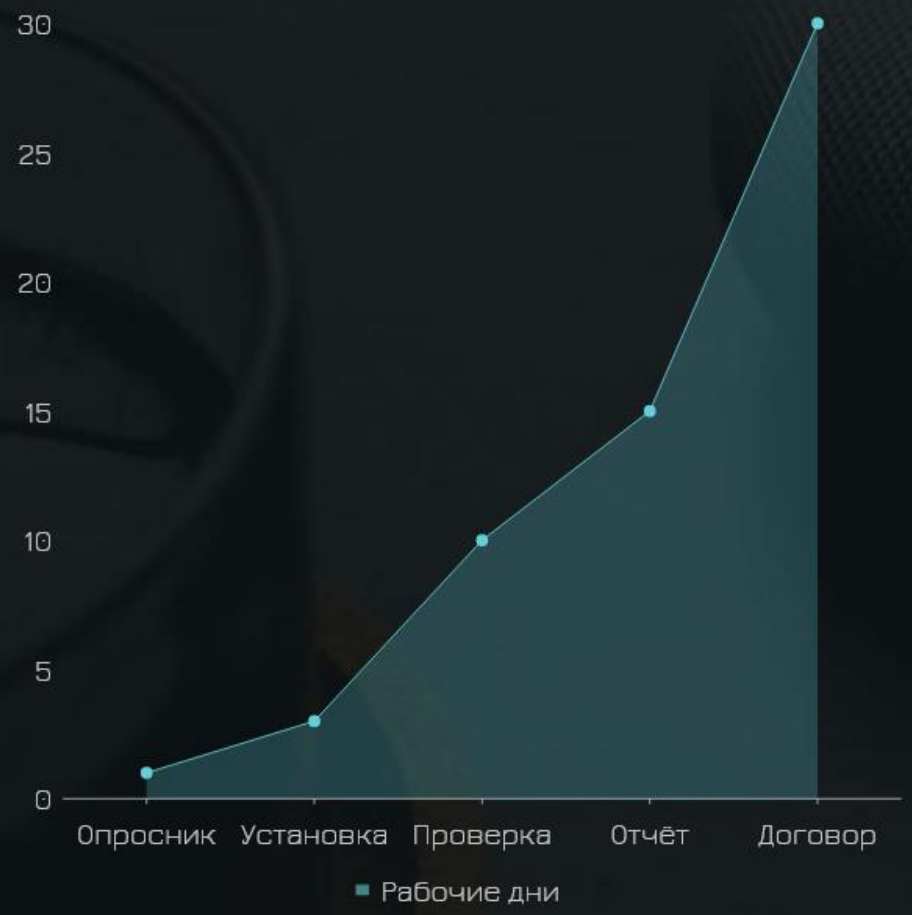
Локализация

- работает локально
- не передает в Интернет
- Ваши пароли останутся у Вас

Простота, безопасность

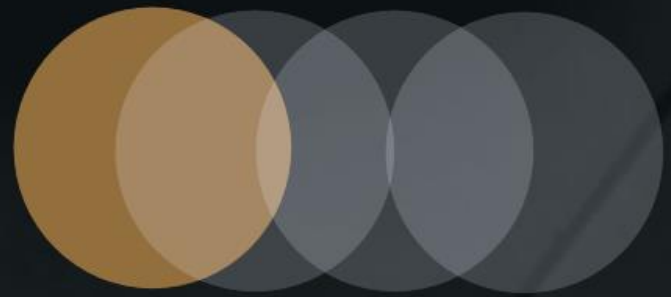
- нет доступа к паролям
- не требует компетенций

КАК НАЧАТЬ ПОЛЬЗОВАТЬСЯ



ПИЛОТНЫЙ ПРОЕКТ:

- вместе заполняем опросник (10 мин.)
- направляем ссылку на ПО
- проводите проверку
- выдаём отчёт, рекомендации, КП
- заключаем договор



База паролей

Содержит 23 972 356 815 записей реальных паролей, в т.ч., имеются 27-символьные утекшие пароли!

БОНУС 1 (из 3).

Примеры сценариев хакеров

Сценарий 1

Попытка использования заводских логина и пароля для доступа к интерфейсу сетевых и др. устройств

Сценарий 2

Использование уязвимости CWE-203 даёт возможность проводить перебор пользователей и подбор паролей в CMS Wordpress

Сценарий 3

Админ-инсайдер, зная целевые аккаунты, обходит защиту и подбирает пароли. Получает доступ к конфиденциальным данным (1С, базы)

Сценарий 4

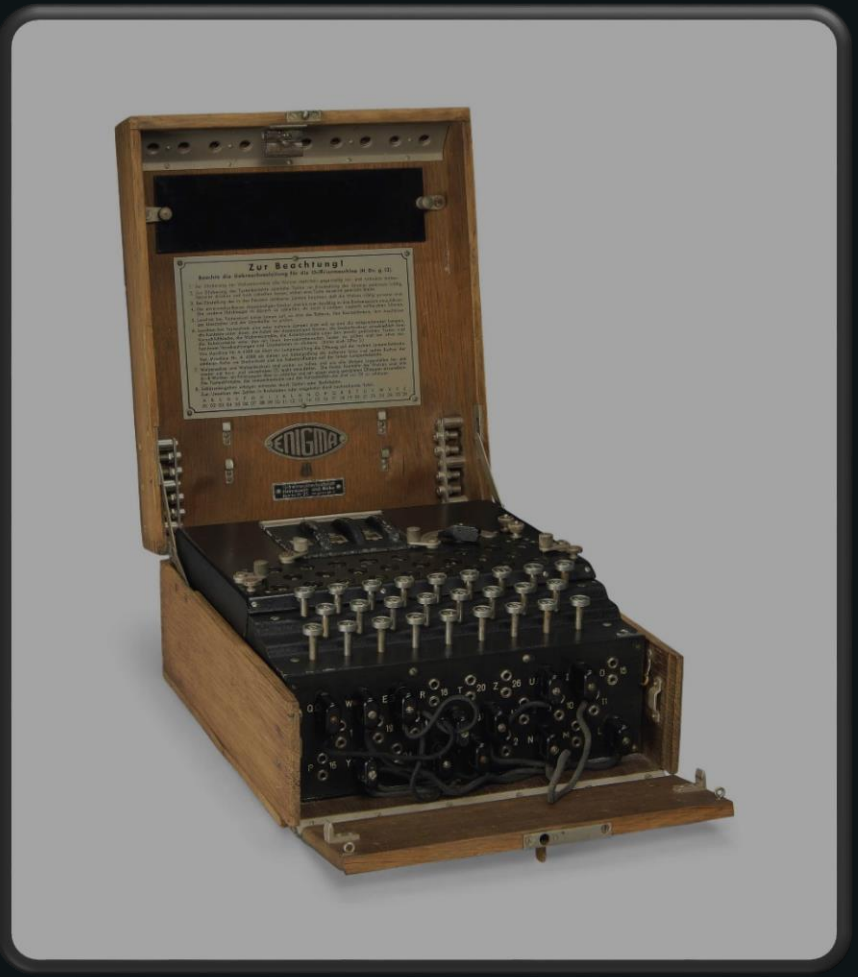
CAPTCHA можно обойти, если взаимодействовать с бэкендом напрямую. Можно подбирать пароль, не встречая препятствий со стороны CAPTCHA

Сценарий 5

Уязвимость: учетки с публичным доменом (*gmail, *yandex), используемые для входа в корпоративные сервисы. Поиск среди утечек и подбор по словарю паролей.

Сценарий 6

Поиск аккаунтов с нужным доменом OSINT (сайт и т.д.), добавление в список типовых учеток админа (root, admin, Админ и т.д.). Обход механизмов защиты и подбор паролей



БОНУС 2 (из 3).
Возражения коллег

СТРАШЕН ЛИШЬ СЛИВ АДМ.ПАРОЛЯ

Если хакер завладел аккаунтом пользователя, он будет использован для продвижения по инфраструктуре и захвата аккаунта администратора

МЫ МЕНЯЕМ ПАРОЛИ КАЖДЫЕ X ДНЕЙ!

Это не убережет от того, что новый введенный пароль уже слабый и содержится в базе утекших. Т.е., даже при смене новый пароль подвержен подбору

МЫ ИСПОЛЬЗУЕМ СЛОЖНЫЕ ПАРОЛИ!

В базах есть и пароли 27 симв. Утекли из-за недостатков защиты, а не из-за нестойкости к подбору. Сильный пароль - и сложный, и отсутствующий в базах

НЕТ ВЫХОДА В ИНТЕРНЕТ

Преодолев периметр, хакер может взломать, в т.ч., АРМ, не подключенные к сети Интернет, т.к. он получил доступ во внутреннюю сеть фирмы.

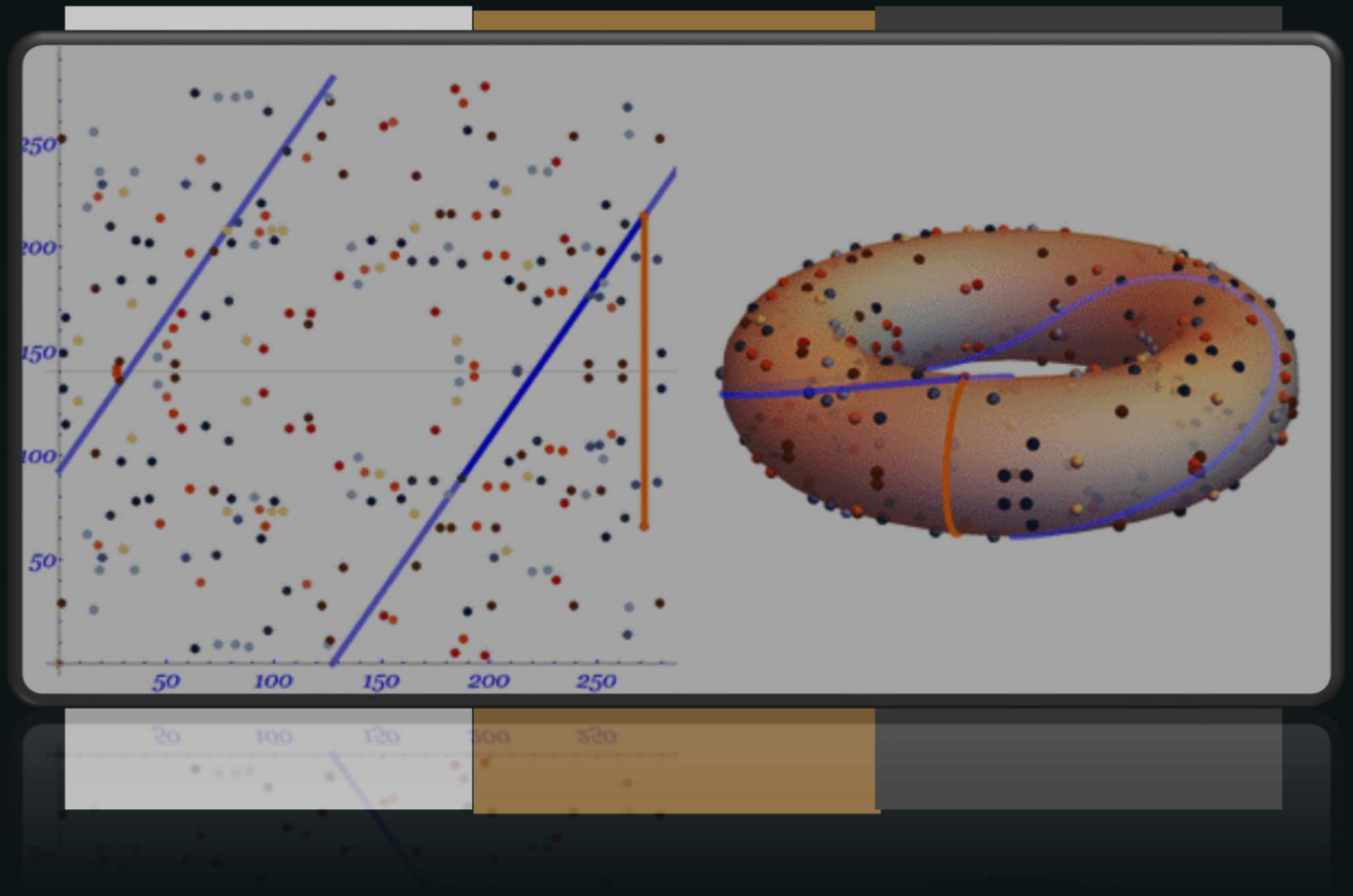
ОГРАНИЧЕНИЕ ПОПЫТОК ВВОДА!

Метод считается надежным, но используется не везде. Существуют методы обхода, когда пароль подбирается не через страницу авторизации

ИБ НА НАЧАЛЬНОЙ СТАДИИ РАЗВИТИЯ

Тем лучше для хакеров. Если не установлены средства защиты, укрепление парольной безопасности - бюджетное и эффективное средство борьбы.

БОНУС 3 (из 3). Бесплатный генератор паролей (ССЫЛКА)



Описание

Использование верхнего и нижнего регистров, цифр и спецсимволов.
Установка длины пароля: 8 - 25 символов
Установка числа паролей для генерации: 1 - 30 шт.

Контакты

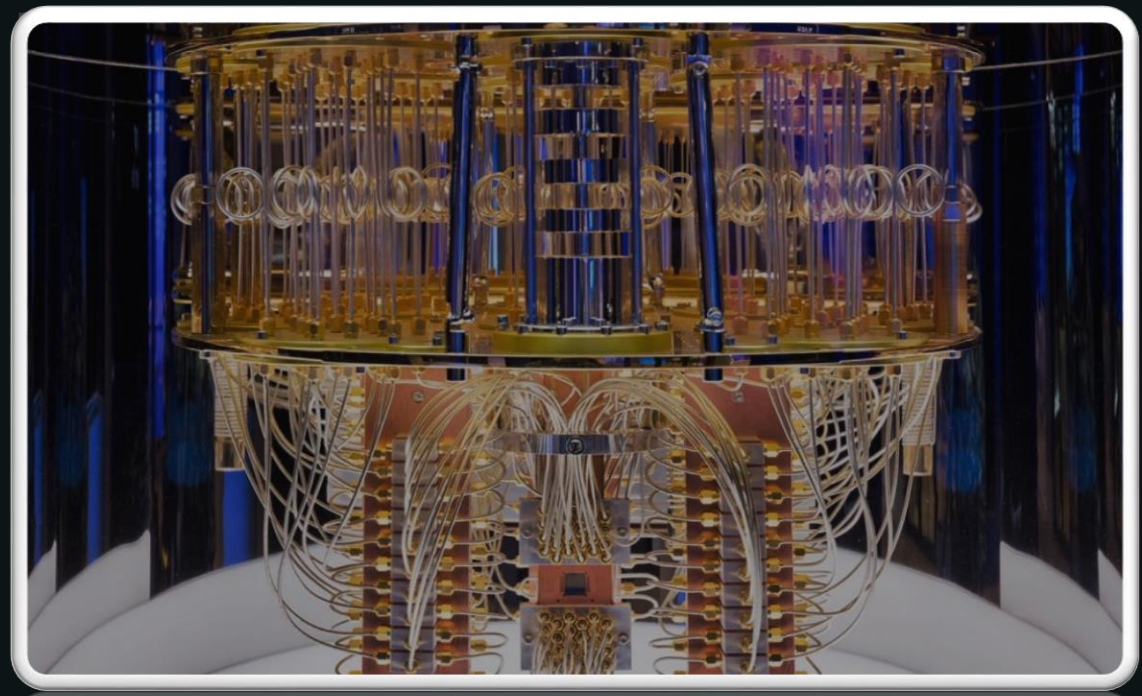
Общество с ограниченной ответственностью "КИБЕРТЕСТ"

Генеральный директор Руденко Дмитрий Олегович

Эл. почта: rudenko.dmitry@kibertest.tech

web-сайт: www.kibertest.tech

Телефон: +7 (927) 531-72-36



СПАСИБО!

По настоящему я осознал незащищенность своих систем, когда при просмотре очередного боевика главный герой, отключая охранную систему, ввел мой пароль!