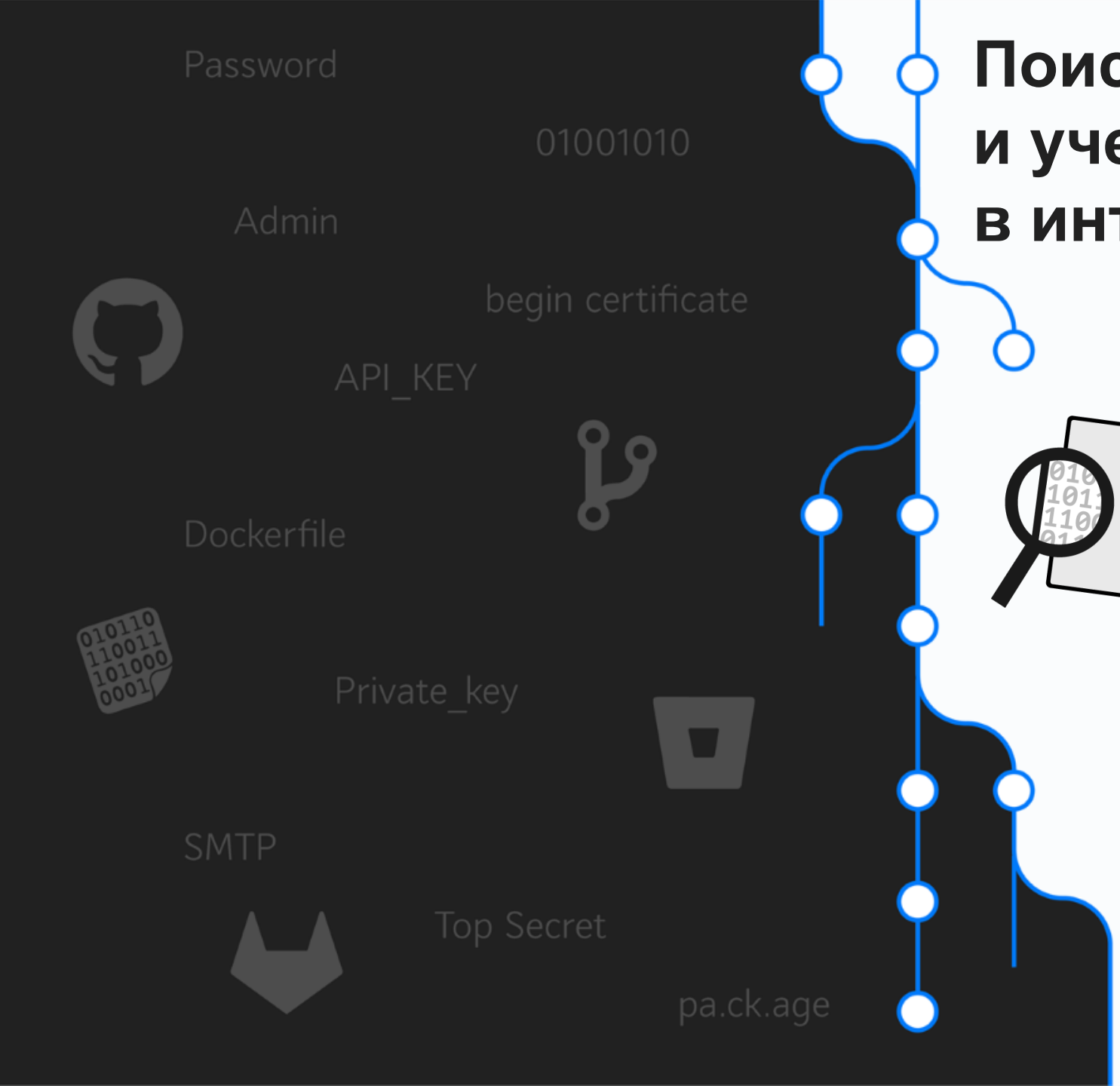


Поиск утечек исходного кода и учетных данных в интернет

LEAK-SEARCH

FIND YOUR LEAKS

Бастриков Антон

Руководитель направления по работе с партнерами

powered by QIWI

Актуальные вопросы

Утечка — некто получает неправомерный доступ к данным

Какие данные утекли?

Кто виноват?

Как и когда произошла утечка?

Что делать?

Конфиденциальные данные —

это любые сведения, доступ к которым ограничен законодательством: ПДн, информация, составляющая профессиональную, коммерческую, служебную и государственную тайну

Технологически – это учетные данные, предоставляющие доступ к системам или БД компании

Например:

- Ключи API
- Логины / пароли пользователей
- Сертификаты безопасности

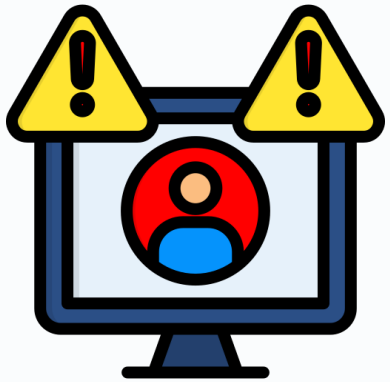
Утечка таких данных может привести к экономическим, интеллектуальным и репутационным рискам

Виды конфиденциальной информации *отличаются многообразием и спецификой обработки. Оптимально руководствоваться нормативными актами для корректного оперирования терминами и практического использования нормативов на практике - 149-ФЗ от 27.07.2006, 152-ФЗ от 27.07.2006, 98-ФЗ от 29.07.2004, 63-ФЗ от 6.04.2011, 187-ФЗ от*

Акторы: случайный инсайдер

Работал в организации и имел слишком большие привилегии:

- Данные оказались в поле зрения случайно или вследствие нездорового любопытства
- Не было злого умысла
- Раскрытая информация не представляет особой угрозы
- Но меры по устранению проблемы предпринять необходимо!



Акторы: злонамеренный инсайдер

Работал в организации и имел слишком большие привилегии:

- У актора были нечистоплотные помыслы
- Существовал мотив, например, месть или получение личной выгоды
- Утёкшие данные могут нанести ущерб организации
- Меры по устранению проблемы обязательны!

Акторы: внешний злоумышленник

Любой злоумышленник, который получает неправомерный доступ к информации:

- Люди с разной мотивацией: от скучающего тинэйджера и заканчивая группой хакеров
- Высший уровень угрозы: проникновения могут быть неоднократными
- Утёкшие данные могут нанести ущерб организации
- Меры по устранению проблемы обязательны!

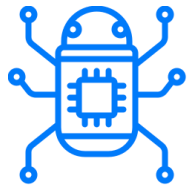
Причины утечки данных

Уязвимости
в системе

Слабые или повторно
используемые пароли

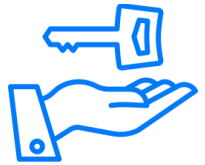
Целевые
атаки

Избыточные права
доступа



Вредоносные
программы

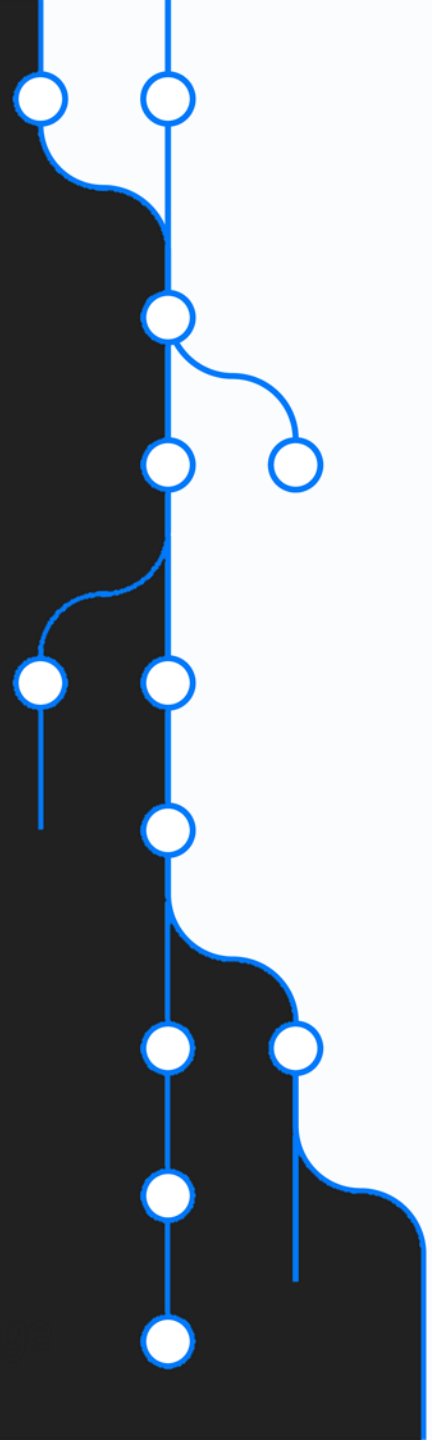
Фишинг или
спуфинг



Украденные учетные
записи

Уязвимости в системе

Компьютер или система часто подвержены атакам разного рода из уязвимости в коде



Злоумышленники намеренно используют известные эксплоиты там, где обновления еще не установлены, что приводит к взлому и утечкам

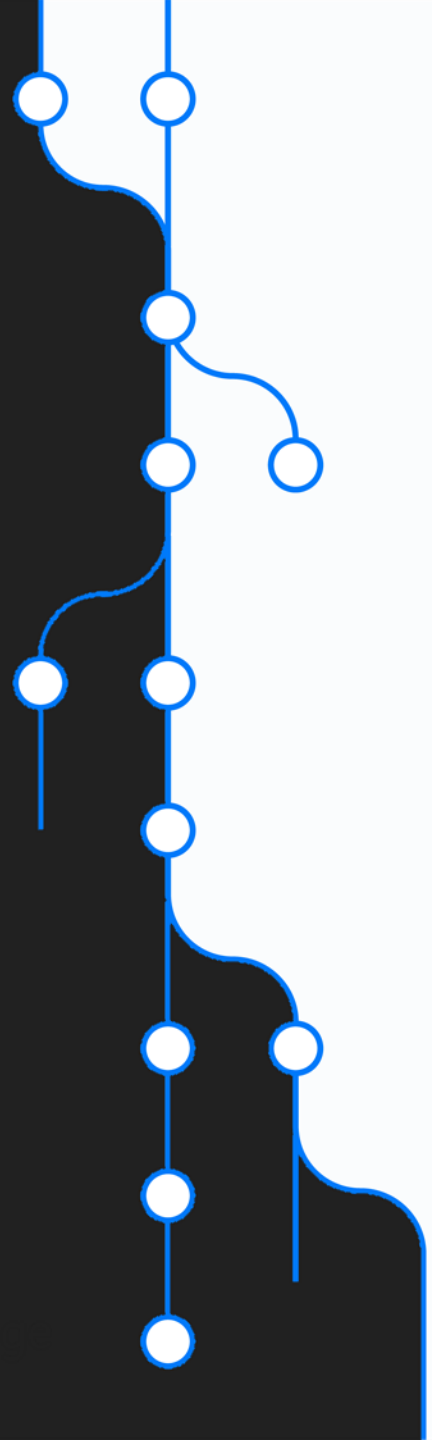
Слабые или повторно используемые пароли

Компрометация паролей, устойчивых ко взлому

Если сотрудники используют корпоративную почту для регистрации на сетевых ресурсах, злоумышленники могут выкрасть данные и получить доступ к корпоративной информации

Целевые атаки

Атаки с нестандартными сценариями, направленные на конкретную организацию



Могут включать техники, начиная от выступления от имени коллеги по работе для получения ценной информации и заканчивая отсылкой поддельных писем конкретным сотрудникам

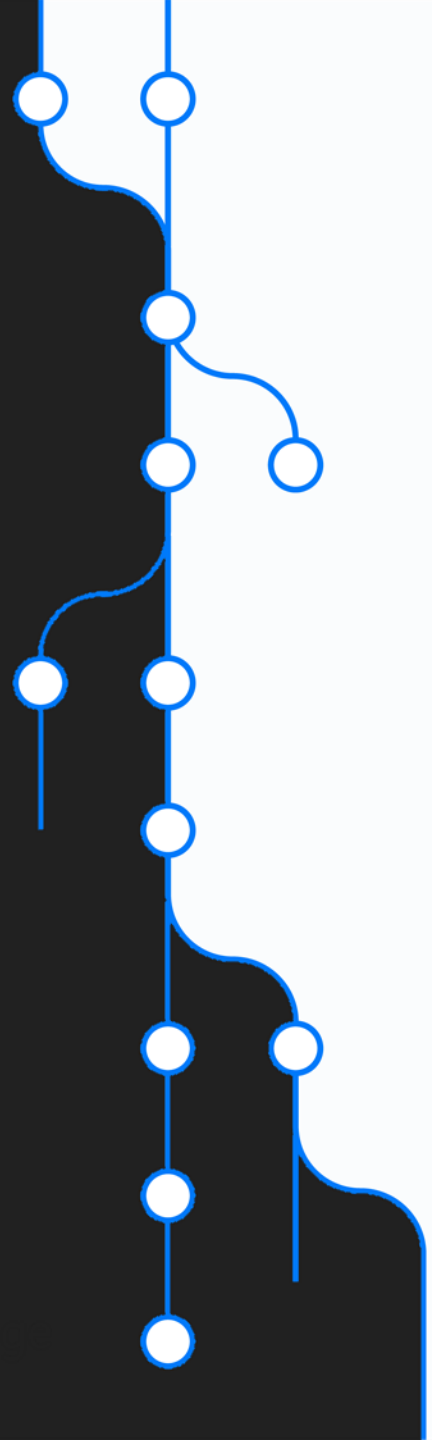
Избыточные права доступа

Ситуации чаще всего возникают, когда у сотрудника меняется роль, или права нового сотрудника наследуются от кого-то еще

Сотрудники, обладающие избыточными правами, могут послужить причиной утечки данных — случайной или намеренной

Вредоносные программы

Инфицирование происходит разными методами, обычно через вложения в письма или вредоносные ссылки



У злоумышленника появляется неограниченный доступ к системе, который используется для дальнейшего перемещения внутрь сети

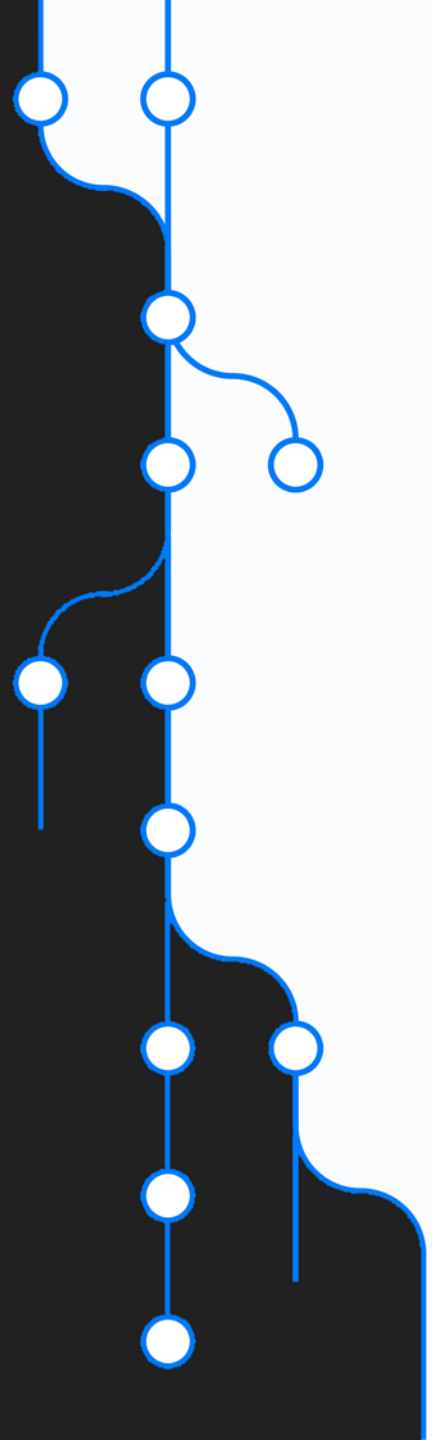
Фишинг или спуфинг

Злонамеренная рассылка электронных писем от имени достоверного источника

Цель — провоцирование жертвы на нажатие вредоносной ссылки, загрузку файла с вредоносом или вовлечение в мошеннические схемы

Украденные учетные записи

Обычно добываются посредством фишинга и авторизации на поддельной странице



Поскольку большинство людей повторно используют пароли, украденная учетная запись потенциально может быть использована для доступа к нескольким сервисам

Как минимизировать риски утечки информации?

Внедрение политики безопасности

Принцип наименьших привилегий

Корпоративная политика паролей

Обучение сотрудников

Leak-Search: сервис поиска утечек

Leak-Search осуществляет мониторинг публичных репозиториев
в интернет и Telegram-каналах на наличие утечек исходного кода,
конфигураций, УЗ, ПДн и других чувствительных данных

Ведет мониторинг использования систем совместной работы в интернете
(в части совместной разработки исходного кода)

Веб-сервис, работающий по модели SaaS (Software as a Service)
в режиме 24/7 и не требующий установки ПО в инфраструктуре клиента

Работает с платформами:

Особенности Leak-Search

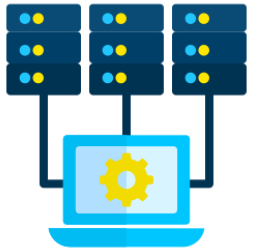
- Интуитивно понятный веб-интерфейс
- Единовременный запуск нескольких задач
- Статистика и отчеты для анализа
- Автоматизация ручного поиска – имитация поиска живым человеком
- Реагирование на изменения в функциональности источников и регулярные обновления сервиса

* Запись в реестре №12874 от 21.02.2022 произведена на основании поручения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 21.02.2022 по протоколу заседания экспертного совета от 14.02.2022 №217пр

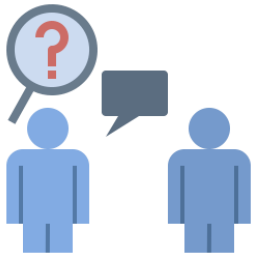
https://reestr.digital.gov.ru/reestr/546103/

Leak-Search позволяет:

Узнать, какие данные утекли



Узнать, куда утекла информация



Определить нарушителей и каналы утечки

Собрать информацию для анализа и выработки мер

Уже используют Leak-Search

Бастриков Антон

Руководитель направления по работе с партнерами

sales@leak-search.com

+7 (916) 501-71-28

Жендаева Виктория

Менеджер продукта

support@leak-search.com

+7 (917) 504-71-92

https://leak-search.com

LEAK-SEARCH
FIND YOUR LEAKS

powered by QIWI