

СЕРВИС ПО МОНИТОРИНГУ УТЕЧЕК ДАННЫХ ДИ ЭЛ БИ АЙ

DLBI - DataLeakage & Breach Intelligence



01

Основное предназначение сервиса мониторинга утечек данных DLBI

Своевременное обнаружение утечек и оповещение ваших клиентов, пользователей и сотрудников о компрометации их телефонов, паролей, электронной почты для предотвращения взлома систем, кражи данных и денежных средств.

02

Более 20 лет команда DLBI занимается информационной безопасностью

Около 36 миллиардов строк из утечек, содержащих пароли, мы проверили и идентифицировали с 2019 года. Порядка 7 миллиардов уникальных пар - логин/пароль проанализированы.

03

Действующая в режиме реального времени

широчайшая сеть мониторинга интернета и даркнета позволяет обнаруживать утечки раньше, чем они станут доступны участникам профессионального сообщества и, тем более, до того, как информация попадет в публичное поле.



ЧТО ПРОИСХОДИТ



Число **хакерских атак** и инсайдерских утечек постоянно **растет** и увеличилось на порядок сегодня. 67 крупных утечек персональных данных произошло за первую половину 2023 года. Объем утекших данных составил 43,6 млн уникальных адресов эл. почты и 47,7 млн телефонов. Также пострадал от утечек и медицинский сектор.



Возможность «расшифровки» (восстановления) и анализа сразу нескольких паролей, принадлежащих одному и тому же человеку, позволяет с **вероятностью более 70%** определить используемые им принципы запоминания кодовой информации, а затем достаточно быстро **подобрать его пароль** для любого ресурса.



Хакеры активно используют **утекшие учетные записи** для взлома различных ресурсов компаний. Пробуют подставлять логины из одних утечек к другим ресурсам.



С развитием интернет-продаж и ростом числа удаленных сотрудников, российские компании вынуждены **переводить все больше процессов в цифру**.



Для **обеспечения защиты** требуется постоянно внедрять новейшие **системы защиты**, что особенно сложно при использовании распределенных и облачных сервисов.



Регулятивное давление постоянно растет и увеличиваются **штрафы за утечки данных**.

МЫ ПРЕДЛАГАЕМ РЕШЕНИЕ

- Автоматизированный мониторинг скомпрометированных учетных записей. Возможность интеграции сервиса DLBI с корпоративными системами заказчика посредством нашего программного интерфейса приложения - API позволяет принимать на вход телефоны, мейлы и логины и выдавать название утечки, дату и пароли. Основное предназначение - оповещение пользователей о компрометации их паролей, во избежание дальнейших инцидентов. API позволяет проверить логин (e-mail или телефон) в нашей крупнейшей в Рунете базе утечек которую мы оперативно и регулярно обновляем на основе мониторинга.
- Экспертное определение актуальности предложений в целях определения достоверности предлагаемых сведений.
- Мониторинг скомпрометированных учетных записей заказчика – поиск в опубликованных утечках и агрегированных массивах учетных записей, данных, относящихся к информационным системам заказчика (почтовым адресам, доменам и другим).
- Мониторинг площадок DarkNet-а на предмет утечки корпоративных баз данных и внутренней информации заказчика – постоянный контроль теневых торговых площадок, Telegram-каналов и закрытых форумов на случай появления на них информации из корпоративных систем заказчика и персональных данных его клиентов. Включает также подготовку и постоянное обновление списка признаков (форматов данных, ключевых слов и др), указывающих на принадлежность информации





Подписывайтесь на наш
telegram-канал
“Утечки информации”
@dataleak

Олеся Ярмоленко Olesya@dlbi.ru