DeviceLock DLP
Proactive Endpoint Security

РАЗВЕДКА УЯЗВИМОСТЕЙ ХРАНЕНИЯ ДАННЫХ

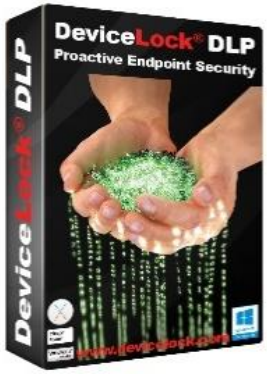
DEVICELOCK DATA BREACH INTELLIGENCE

СЕРГЕЙ ВАХОНИН
Директор по решениям
EMAIL SV@DEVICELOCK.COM

АШОТ ОГАНЕСЯН
Технический директор, основатель
EMAIL ASHOT@DEVICELOCK.COM

АО Смарт Лайн Инк
Москва, 2019

DeviceLock - 20 лет на рынке ИБ всего мира



ПЕРВАЯ ВЕРСИЯ
DEVICELOCK -
1996

Продукт

Программный комплекс **DeviceLock DLP**

Система защиты информации для организаций, которым необходимо простое и доступное решение по предотвращению утечек данных с корпоративных компьютеров под управлением Windows и MacOS, а также виртуализованных рабочих сред и приложений Windows.

Смарт Лайн Инк / DeviceLock, Inc.

Отечественная компания с штаб-квартирой и офисом разработки **в Москве** (АО «Смарт Лайн Инк),
офисами продаж в США (DeviceLock NA, San Ramon, California), Канаде (DeviceLock Canada, North Vancouver), Великобритании (DeviceLock UK, London), Германии (DeviceLock Europe GmbH, Ratingen), Италии (DeviceLock Italy, Milan),
а также партнерской сетью по всему миру.

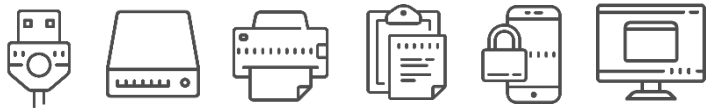
Более 70 000 пользователей при более чем 7 000 000 инсталляций по всему миру

DeviceLock - 20 лет на рынке ИБ всего мира

DeviceLock DLP

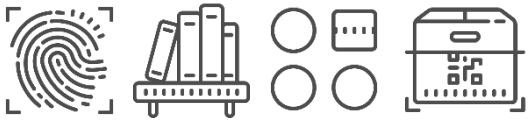
ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

… все устройства и интерфейсы



…каналы сетевых коммуникаций

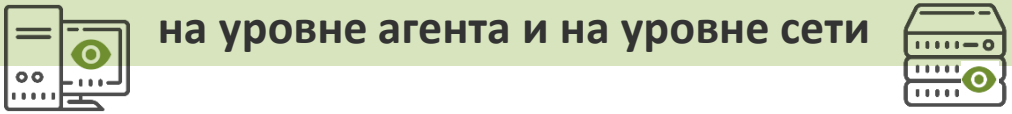
…с применением технологий контентной фильтрации



в режиме реального времени, в любых сценариях!

ДЕТАЛЬНЫЙ МОНИТОРИНГ СОБЫТИЙ

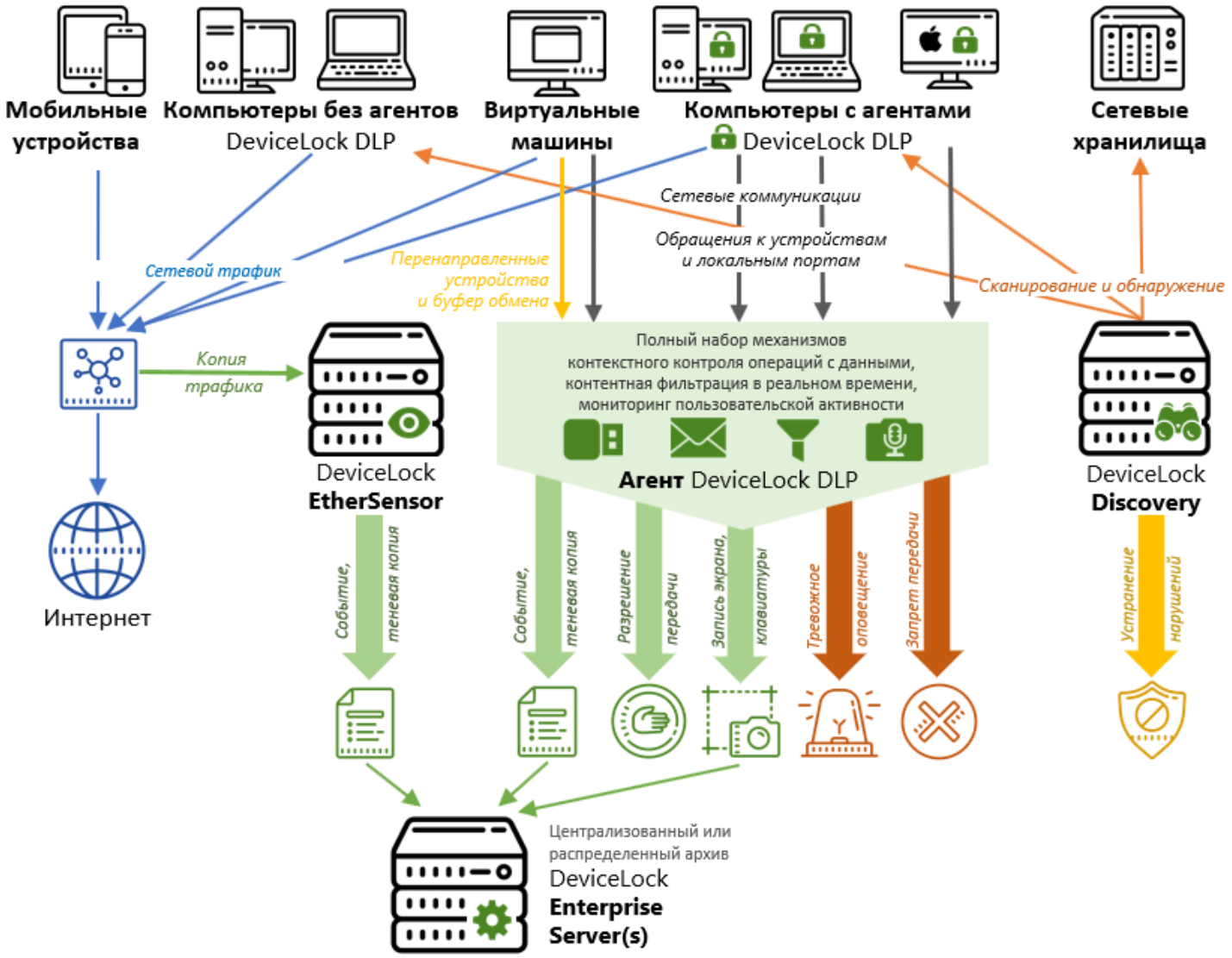
на уровне агента и на уровне сети



СКАНИРОВАНИЕ ХРАНИМЫХ ДАННЫХ

АНАЛИЗ АРХИВА: СЕРВЕР ПОЛНОТЕКСТОВОГО ПОИСКА

DeviceLock DLP в одной картинке



КАК ОБНАРУЖИВАЮТ “ОТКРЫТЫЕ” БАЗЫ ДАННЫХ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ.

АШОТ ОГАНЕСЯН

Технический директор, основатель DeviceLock

EMAIL ASHOT@DEVICELOCK.COM

Статистика

Все обнаруженные базы MongoDB

TOTAL RESULTS

65,076

TOP COUNTRIES

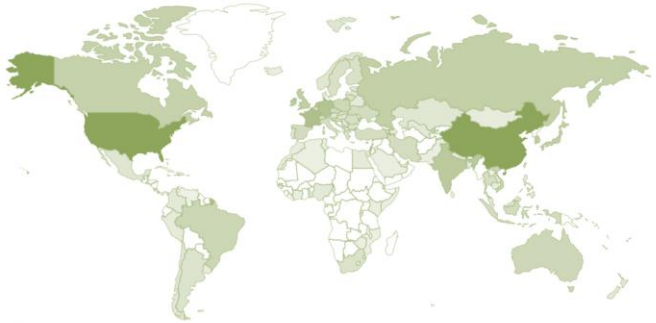
United States	22,706
China	11,138
Germany	3,861
France	3,387
Singapore	2,743

Все обнаруженные базы Elasticsearch

TOTAL RESULTS

28,488

TOP COUNTRIES



United States	8,801
China	8,757
France	1,622
Germany	1,116
Netherlands	1,082

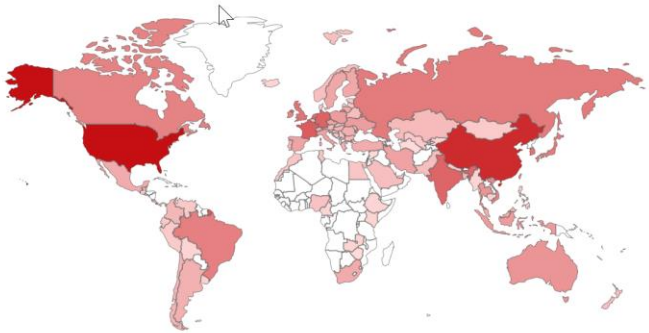
Статистика

Незащищенные базы MongoDB

TOTAL RESULTS

21,332

TOP COUNTRIES



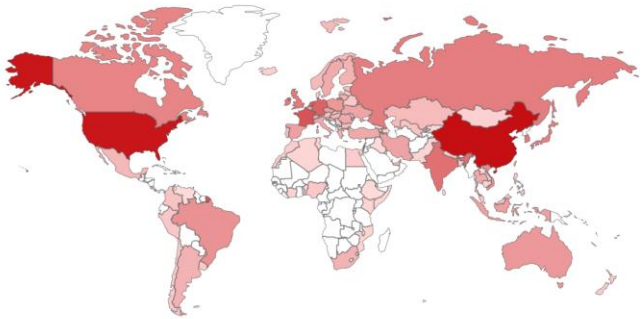
United States	7,485
China	4,125
France	1,127
Germany	923
Singapore	840

Незащищенные базы Elasticsearch

TOTAL RESULTS

20,747

TOP COUNTRIES

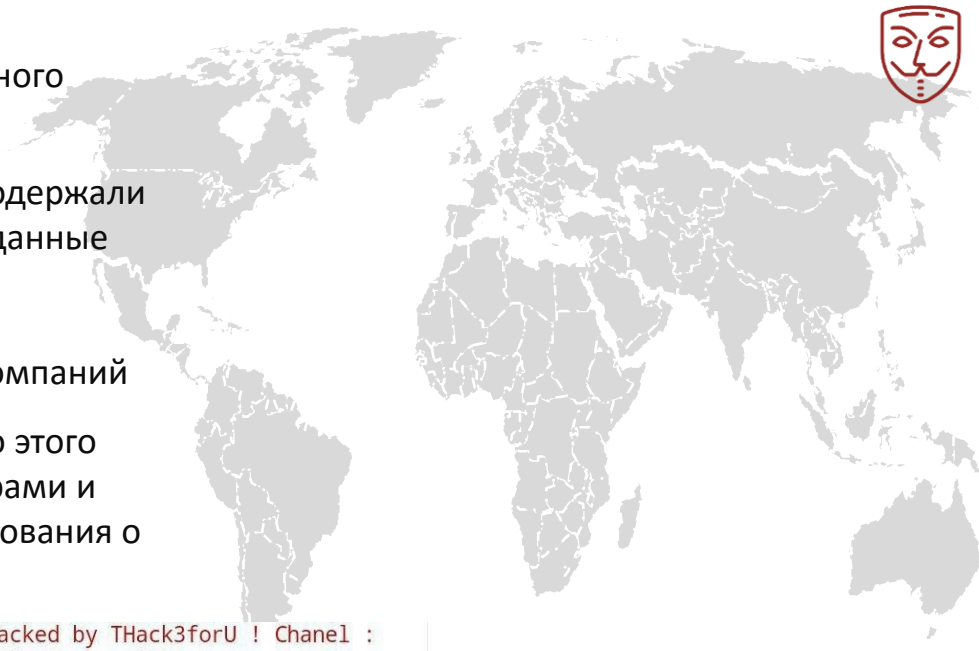


China	6,712
United States	5,774
France	1,301
Netherlands	902
Germany	837

Статистика

С начала 2019 в Рунете обследовано более 2300 серверов, использующих платформы MongoDB, Elasticsearch и Yandex ClickHouse

- 52% предоставляли возможность неавторизованного доступа
- 10% при этом содержали персональные данные россиян или коммерческую информацию компаний
- Еще 4% были до этого взломаны хакерами и уже имели требования о выкупе



```
5   "Message": "Hacked by THack3forU ! Chanel :
http://t.me/UkraineHack\nТільки ворог, що
сміється…\nСмійся, лютий враже!\nТа не дуже, бо
все гине,\n— Слава не поляже;\nНе поляже, а
розкаже,\nЩо діялось в світі,\nЧия правда, чия
кривда\nІ чиї ми діти."
```

В начале мая выяснилось, что хакеры группировки Unistellar уничтожили данные 12,5 тысяч "открытых" баз MongoDB

В России находится более 230 серверов с MongoDB, подвергшихся этой атаке

@dataleak – канал со свежайшей информацией. Все основное – там!

Статистика

В мире

- Более 21 тыс. “открытых” MongoDB
- Более 20 тыс. “открытых” Elasticsearch

В России *

Q2 2019	Всего	Без аутентификации	Зараженные	Обнаружено критичное содержимое (персональные, медицинские и т.п. данные)
MongoDB	1610	608	272	20
Elasticsearch	724	605	72	28

** Данные собственного исследования DeviceLock*

Почему это происходит?

MongoД.Б!

- Кривые руки внедренцев/администраторов и даже разработчиков.
- По умолчанию MongoDB не имеет аутентификации – забывают устанавливать пароль на доступ и не закрывают доступ к внутренним базам на файрволлах
- Реальный случай с Elasticsearch, дословно со слов потерпевшего:
  “прикручиваем Эластик к серверу и как оказалось, докер добавляет свои правила в iptables, которые перекрыли ручную настройку правил на уровне Elastic. Как следствие, эти порты были доступны всему интернету (о чем мы и не подозревали). ”

Как искать?

1. **Shodan** – попса, каждый школьник уже знает.
   Отлично работает, удобное API!
2. **BinaryEdge** – дает больше результатов, на 90% пересекается с Shodan.
   Часто находится что-то новое.
3. **Censys** – что-то среднее по результатам выдачи между Shodan и BinaryEdge.
4. **Zoomeye** (Китай) – честно не смог использовать, лучше знать китайский – часто вылезает, даже на этапе регистрации ;)

Простейшие примеры запросов в поисковой строке:

BinaryEdge
elasticsearch.docs:>1
mongodb.totalSize:>1

Shodan
port:"9200" all:"elastic indices“
all:"mongodb server information" all:"metrics“

Censys
protocols: "9200/elasticsearch“
protocols: "27017/mongodb"

Основная «сила» поиска - доступ через API.

Необходим токен доступа к API.

Есть готовые скрипты на Питоне типа leaklooker.py

Мощный OSINT-инструмент - Lampyre. Интеграция с Shodan (обещали BinaryEdge, но только после релиза). Удобно смотреть статистику обхода Shodan, строить граф связей и находить владельцев баз.

Команда "show log" в консоли MongoDB - показывает лог доступа, можно смотреть, с каких IP-адресов подключались и что делали. Помогает для выявления владельца базы.

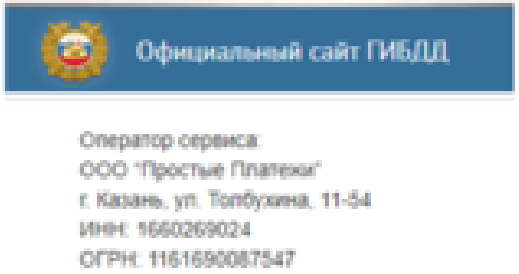
ПОДРОБНЕЕ В МОЕЙ СТАТЬЕ (опубликовано в корпоративном блоге)
https://www.devicelock.com/ru/blog/obnaruzhenie-otkrytyh-baz-dannyh-mongodb-i-elasticsearch.html

Самые громкие кейсы

- С начала года обнаружено более 50 значимых (крупных) баз
- Паттерн в 90% утечек Elastic и ClickHouse – логи ИС, которые содержат чувствительные данные
- Mongo – просто база с дефолтными (никакими) настройками аутентификации

- **DOC+** - Медицинский сервис. Обнаружена «открытая» база данных ClickHouse, содержащая персональные данные сотрудников, информацию о местоположении пользователей DOC+, их IP-адреса и т.п. Используя токен (API_USER_TOKEN) пользователя, можно получить его персональные данные. Доступ закрыт в течение суток. Получен официальный ответ.
- **Finservice PRO** – кредитный брокер. В обнаруженной базе данных содержалась информация о ~300 тыс. заемщиков и более 819 тыс. отсканированных документов. Доступ закрыт через сутки. Ответа не было.
- **Клаустрофобия** – оффлайн-квесты. Обнаружена база данных Elasticsearch с заказами квестов. В базе более 1 млн. записей, включая мобильные телефоны, адреса электронной почты, имена и т.п. . Найдены даже фотографии участников квестов. Доступ закрыт оперативно, получен ответ.
- «**Госоплата ГИБДД/ФССП**» – частный платежный сервис. Обнаружены журналы ИС, содержащие подробности платежей и персональные данные. Доступ закрыт в течение суток. Ответа не поступило.
- **Слетать.ру** – сервис по подбору туров. Обнаружены такие данные, как логины и пароли нескольких сотен подключенных к системе туристических агентств, паспортные данные клиентов и информация о билетах. Доступ закрыт в течение нескольких часов после оповещения. Вместо благодарности сервис предпочел выдать неадекватные комментарии в прессу, заявив, что это «заказуха». ☺
- **Радарио** – билетная система. Обнаружены логи ИС, из которых можно было получить персональные данные, логины и пароли пользователей, а также непосредственно сами электронные билеты. Доступ закрыт в течение нескольких часов после оповещения. Сервис прислал благодарность за уведомление.
- **CMD** – сеть медицинских лабораторий. Обнаружены логи ИС, из которых можно было получить персональные данные врачей и клиентов, включая медицинские данные исследований. Доступ закрыт в течение нескольких суток после оповещения. Получен ответ и благодарность за уведомление.

Один раз - недостаточно. Надо два!



Подробные персональные данные пользователей сайтов оплатагибдд.рф, paygibdd.ru, gos-oplata.ru, штрафов.net и oplata-fssp.ru неопределённое время находились в открытом доступе.

В доступе оказались все подробности платежей: номер постановления о штрафе, государственный номерной знак автомобиля, номер исполнительного производства при платеже на сайте службы судебных приставов, первые и последние цифры банковских карт, через какой платёжный сервис произведена оплата и пр.

База содержала в себе логи информационной системы (ИС), а уже в логах и находилась вся подробная информация. Логи хранились только за период начиная с 28.02.2019, а не за все время работы ИС. В некоторых индексах данные были с 17.03.2019. Кроме того, данные платежных карт из платежных шлюзов не передавались в данную ИС, а потому и не сохранялись в ее логах. Поле cardnumber имело вид: 123456********1234. При этом число открытых записей можно оценить в сотни тысяч, только за один день апреля открытыми оказались записи о 40 тыс. платежей.

Впервые база «засветилась» в специализированном поисковом сервере 24.02.2019. Нами она была обнаружена поздно ночью 12.04.2019, уже утром следующего дня мы оповестили пострадавшие сервисы, но ответа не получили. Сервер тихо убрали из открытого доступа 13.04.2019 около 15:20-15:45 (МСК).
Все сервера оплаты услуг - братья-близнецы, управляемые ООО “Простые Платежи”, г. Казань..

21.05.2019 тот же самый (что и первый раз) сервер Elasticsearch, с теми же самыми (плюс новые) индексами снова появляется в открытом доступе!
22.05.2019 в 1:25 мы оповестили владельцев о проблеме и вплоть до утра 24.05 Elasticsearch оставался открытым.
За промежуток с 01.05 по 22.05 в индексах было доступно:

- ✓ 127525 записей в индексе paygibdd
- ✓ 49627 записей в индексе shtrafov-net
- ✓ 162282 записей в индексе oplata-fssp
- ✓ 220201 записей в индексе gosoplata

DeviceLock Data Breach Intelligence

Один из способов избежать утечек корпоративных данных из незащищенных информационных систем - проводить регулярную ревизию своих информационных активов. Чем раньше будет обнаружена уязвимость организации и реализации систем хранения данных в облаках и других хранилищах данных, доступных извне, тем ниже риск обнаружения данных злоумышленниками и последующей утечки.

Сервис **DeviceLock Data Breach Intelligence** включает в себя следующие услуги:

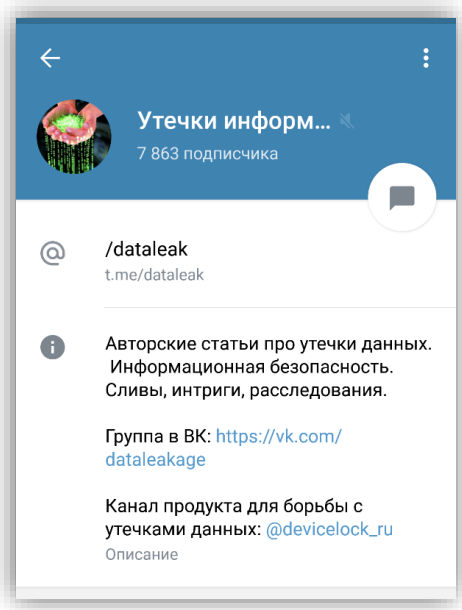
- **Разведка уязвимостей хранения данных** – анализ внешней серверной инфраструктуры Заказчика с выявлением недостатков реализации хранения, в целях обнаружения незащищенных чувствительных данных организации. В частности, проводится выявление и анализ серверов с текущими или архивными данными, журналами ИС и анализ обнаруженных данных на наличие в них чувствительной информации Заказчика (персональные данные, информация с признаками коммерческой тайны, др.). Используется автоматизированная система собственной разработки с элементами искусственного интеллекта, а также ручной анализ данных силами аналитиков
- **Мониторинг предложений о продаже чувствительных данных** Заказчика на различных закрытых площадках, группах Telegram и других мошеннических ресурсах в DarkNet.

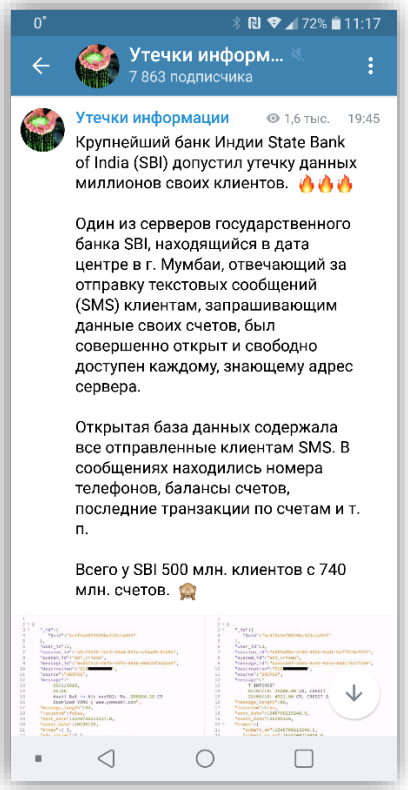
По итогам выполнения работ предоставляется детализированный отчёт с указанием выявленных уязвимостей и фактов компрометации данных, а также рекомендации по их устранению. Также возможно оперативное уведомление непосредственно в момент обнаружения любым удобным для Заказчика способом (по электронной почте, через любой мессенджер).

https://www.devicelock.com/ru/data-breach-intelligence/

СПАСИБО
ЗА ВНИМАНИЕ!

@dataleak





АШОТ ОГАНЕСЯН
ASHOT@DEVICELOCK.COM

www.DeviceLock.com