Федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский университет ИТМО»
Факультет программной инженерии и компьютерной техники

Лабораторная работа №8

«Мини-исследование: Утечка данных и цифровая гигиена»

Дисциплина «Информационная безопасность»

Выполнил:
Студент группы P3431
Нодири Хисравхон

Преподаватель:
Маркина Татьяна Анатольевна

г. Санкт-Петербург
2025г.

Содержание

1 Краткая сводка

По данным проверки адреса в сервисе *Have I Been Pwned*, обнаружено **4** инцидента утечки, затрагивающих мой email.

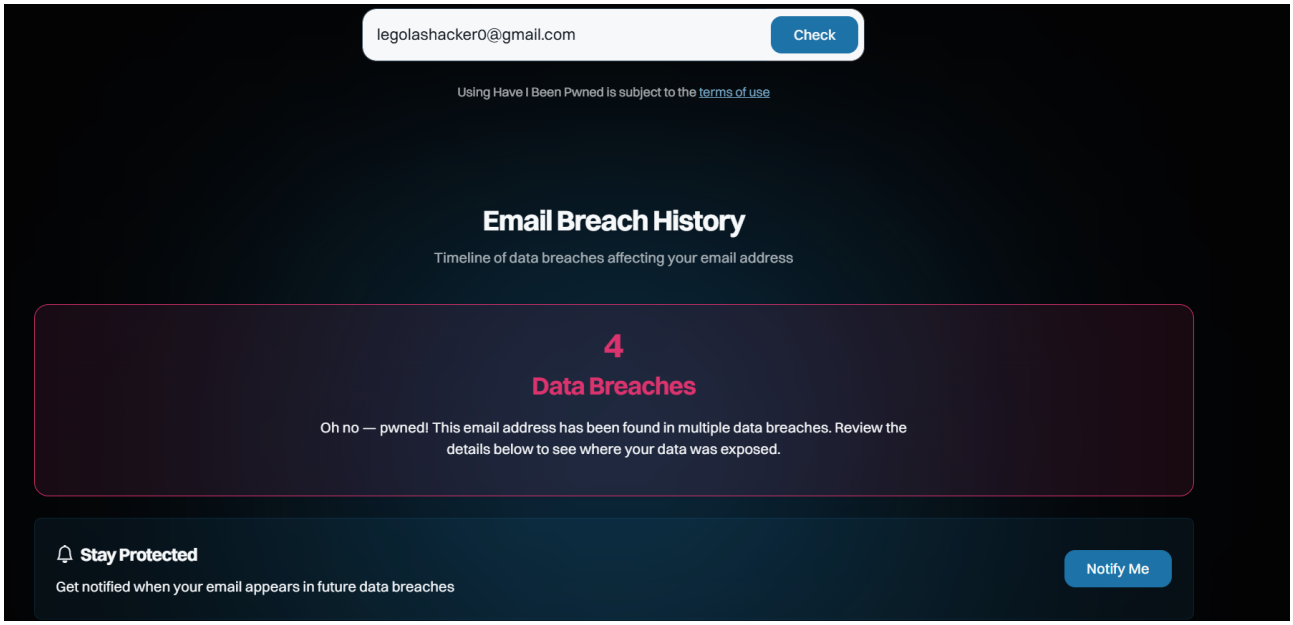

Рис. 1: Сводка: 4 обнаруженные утечки (HIBP)

2 Хронология инцидентов

Aptoide — апрель 2020

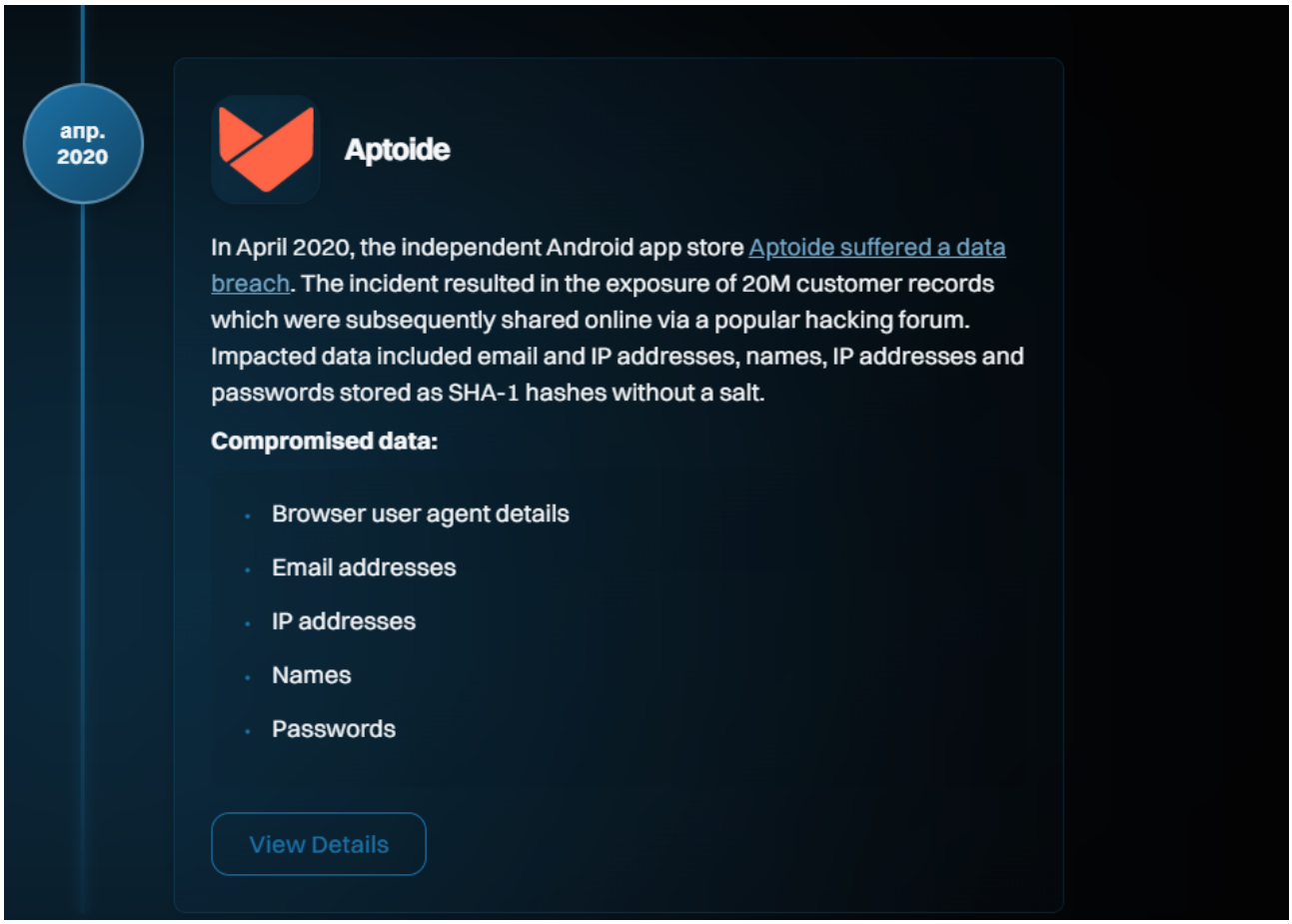

Рис. 2: Aptoide: описание инцидента и перечень полей

Независимый магазин приложений Android. Опубликовано $\sim$ 20 млн записей. Пароли хранились как *SHA-1* без соли, что существенно облегчает их взлом перебором/радужными таблицами.
Скомпрометировано: email, имя, *IP-адрес*, *User-Agent* браузера, пароли (SHA-1 без соли).

Wakanim — август 2022

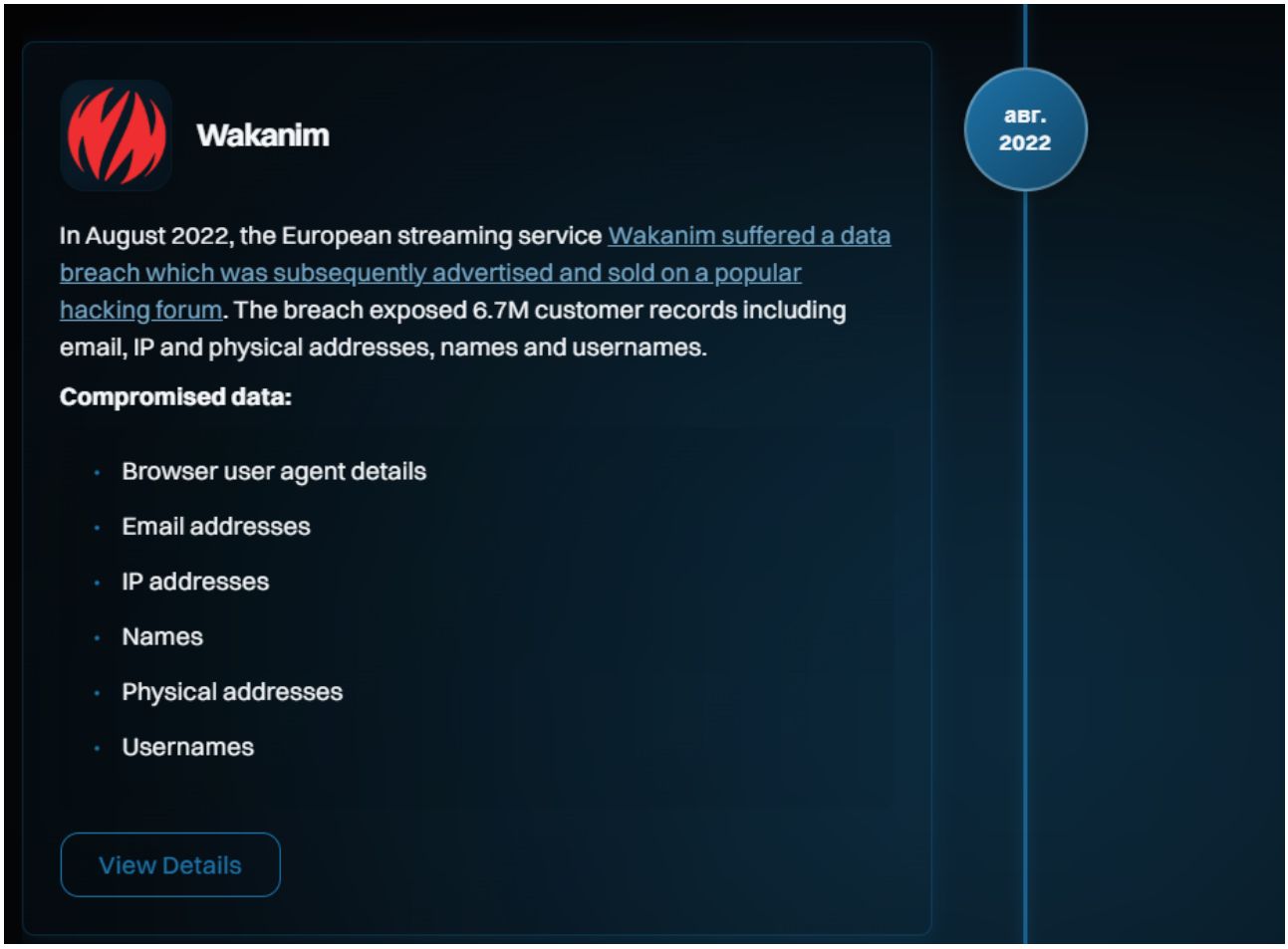

Рис. 3: Wakanim: европейский видеосервис

Европеский стриминг сервис аниме. Утечка $\sim 6{,}7$ млн записей.
Скомпрометировано: email, имя, *имя пользователя*, *IP-адрес*, *User-Agent*, физический адрес.

Chess — ноябрь 2023

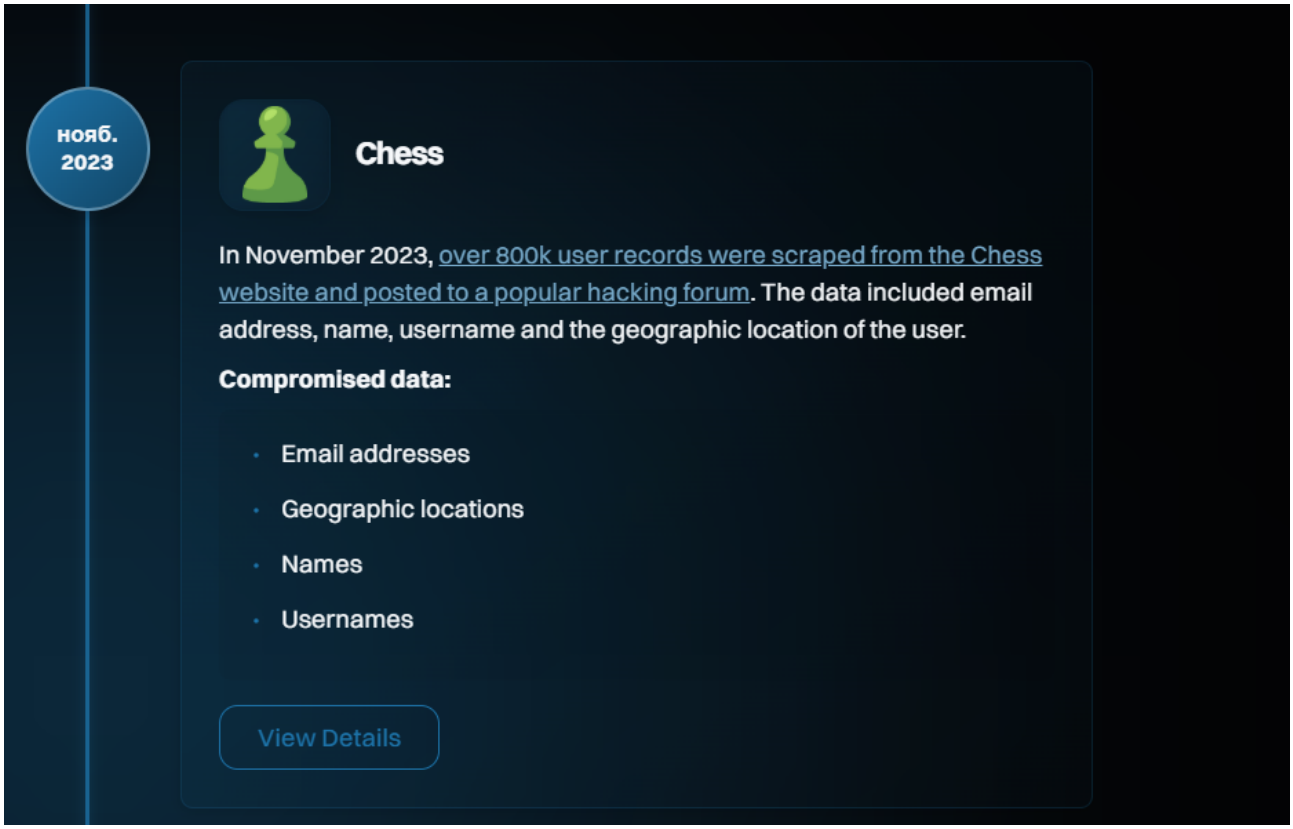

Рис. 4: Chess: выгрузка ∼ 800k записей

Скрейп пользовательских записей. Паролей нет, но есть привязка email к никнейму и географии — наверное это удобно для целевого фишинга.
Скомпрометировано: email, имя, *никнейм/username*, *геолокация* (страна/город).

French Citizens — сентябрь 2024

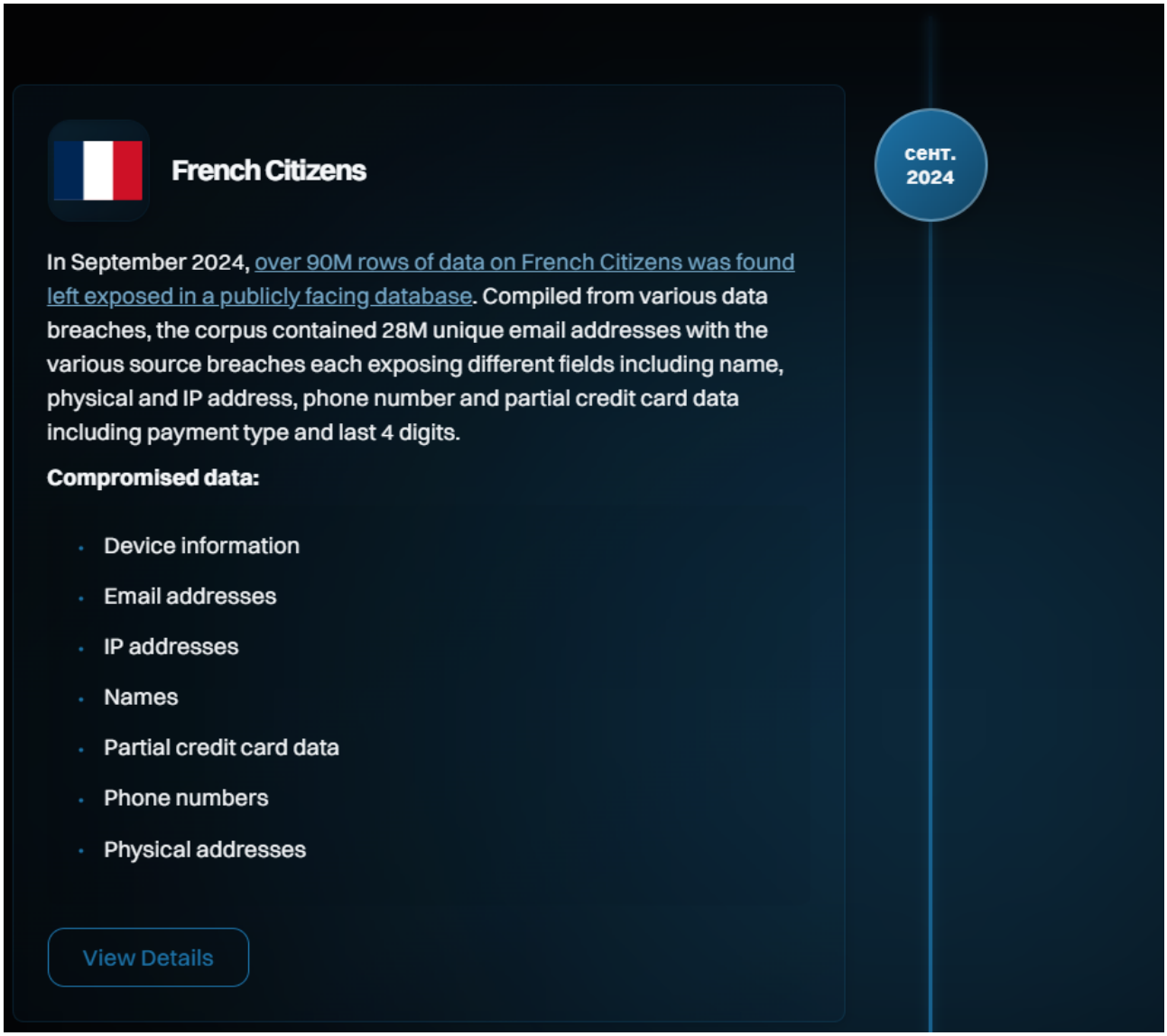

Рис. 5: French Citizens: агрегированная база $>$ 90 млн строк

Сборная база из разных источников, содержала $\sim$ 28 млн уникальных email и *частичные* платёжные данные. Даже последние 4 цифры карты.
Скомпрометировано: email, имя, *IP-адрес*, *инфо об устройстве*, *телефон*, физический адрес, частичные данные карты (тип и последние 4 цифры).

3 Аудит публичной информации

Что видно незнакомцам обо мне:

- **VK**: имя/фамилия, аватар, город/школа/ВУЗ, список друзей (частично), сообщество/лайки, дата рождения, ссылки на другие соцсети.
- **Telegram**: username, фото профиля, био/описание, публичные каналы и комментарии, активность в группах (если публичные), время последней активности.
- **Прочее** (Discord, GitHub, Steam): никнейм, часовой пояс/страна, играемое сейчас, публичные репозитории (почта в git-коммитах), список друзей/сообществ, ссылки на сайты.

4 Личные правила цифровой гигиены

1. **Один логин — один пароль.** Никогда не повторяю пароли; использую менеджер паролей и генерирую 14–20 символов.
2. **Везде, где можно — 2FA.** Предпочтение TOTP/аппаратным ключам; SMS — только как запасной вариант.
3. **Две почты и маски.** Отдельный «бытовой» email и «публичный». Для регистраций — алиасы/-маски почты, чтобы быстро «глушить» скомпрометированные логины.
4. **Полугодовой чек-ап приватности.** Раз в 6 месяцев прохожу настройки конфиденциальности VK/Telegram/Google/Apple; чищу старые сессии и разрешения третьим приложениям.
5. **Гигиена устройств.** Автообновления ОС/браузера, расширения только из официальных магазинов, закрытые уведомления на заблокированном экране, шифрование диска и PIN/биометрия.
6. **Осторожность с персональными данными.** Телефон, адрес и платежные данные не передаю в мессенджерах без необходимости; документы — только через защищённые каналы и с маскировкой лишнего.
7. **Анти-фишинг.** Никогда не перехожу по ссылкам из писем/СМС «от банка/доставки» — открываю сайт вручную; для важных сервисов добавлены закладки.