Технологии и медиа , 22 мая, 09:00
0

Эксперты оценили объем попавших в Сеть данных клиентов доставки еды

Эксперты DLBI назвали число пострадавших от утечек данных клиентов сервисов доставки еды
По данным DLBI, только с февраля в Сеть могли утечь данные 8 млн клиентов различных сервисов доставки еды. Оценка не учитывает последний случай, произошедший с Delivery Club, который может побить предыдущие рекорды на этом рынке

С начала февраля по середину мая в открытый доступ попали данные более чем 8 млн пользователей сервисов доставки еды. Такую оценку РБК назвал представитель сервиса DLBI, который занимается изучением утечек данных и мониторингом даркнета.

Крупнейшие утечки данных были зафиксированы у сервисов «Яндекс.Еда» (более 6,8 млн пользователей) и «Два берега» (780 тыс. пользователей). На третьем месте в списке выявленных DLBI утечек — сайт hgclub.ru, принадлежащий оператору популярных ресторанных сетей «Росинтер Ресторантс Холдинг». Предположительно 2 мая в Сеть попали данные 106 тыс. пользователей. Остальные утечки пришлись на региональные сервисы с небольшим количество клиентов, однако подобных утечек было больше десяти.

1 марта сервис «Яндекс.Еда» сообщил об утечке номеров телефонов клиентов и информации об их заказах. Компания объяснила это недобросовестными действиями одного из сотрудников. В связи с этим сервис решил отказаться от ручной обработки информации, связанной с заказами, и уменьшить число сотрудников, которые имеют доступ к персональным данным.

В конце марта в соцсетях начала распространяться ссылка на сайт, на котором были личные данные пользователей «Яндекс.Еды» в виде карты, там были указаны адрес доставки, телефон, электронная почта, сумма заказов за последние полгода. В середине апреля в Замоскворецкий суд Москвы из-за этой утечки поступил коллективный иск от пользователей «Яндекс.Еды». Они требуют компенсацию морального вреда в размере 100 тыс. руб. на каждого и чтобы «Яндекс» в течение месяца с момента вступления решения суда в силу разместил информацию о принятых мерах по обеспечению сохранности персональных данных.

В пятницу, 20 мая, об утечке данных клиентов также сообщил крупнейший сервис доставки еды в России Delivery Club. Число пострадавших пользователей в компании не назвали, лишь сообщили, что утекла информация о заказах без банковских реквизитов.

По информации Telegram-канала In4security, утекшая база заказов Delivery Club содержит 250 млн строк с персональными данными пользователей, включая Ф.И.О., адреса и информацию о заказах. Однако основатель DLBI Ашот Оганесян настаивает, что в выложенном образце около 1 млн строк, содержащих имя, номер телефона (более 827,7 тыс. уникальных номеров), адрес доставки, адрес электронной почты (более 183,8 уникальных), состав заказа и стоимость, IP-адрес (более 507,6 уникальных). Из дат и времени следует, что речь идет о заказах с 24 мая 2020-го по 4 июля 2021 года. «Каков реальный объем клиентских данных во всей базе, сказать сложно, так как экстраполяция доли уникальных пользователей в пробнике дает 50 млн клиентов, что вряд ли возможно. Однако можно говорить, что если реальный объем утечки соответствует заявленным 250 млн строк, то в руки злоумышленников попала большая часть или вся база заказов Delivery Club, и это — крупнейшая утечка из российских служб доставки на данный момент», — рассуждает Оганесян.

По словам главы AVG Legal Алексея Гавришева, компании — операторы персональных данных несут прежде всего репутационные риски при утечке данных своих пользователей. Согласно ст. 13.11 Административного кодекса, за нарушение законодательства в области персональных данных для юрлиц предусмотрен штраф в размере до 100 тыс. руб. Кроме того, клиенты, чьи персональные

данные стали достоянием третьих лиц, могут предъявить компании гражданские иски, и они могут рассчитывать на удовлетворение своих требований, если докажут в суде наличие причинно-следственной связи между утечкой их персональных данных и наступления для них негативных последствий.

Почему растет число утечек

По словам Ашота Оганесяна, рост числа утечек данных пользователей может быть связан, с одной стороны, с падением продаж в сервисах доставки еды и следующим за ним сокращением издержек, как это ранее было с микрофинансовыми организациями, базы которых массово утекали после резкого сокращения этого рынка в 2018–2019 годах. С другой стороны, по его мнению, играет роль разрушение ИТ-инфраструктуры малого бизнеса, для поддержки которой активно использовались западные сервисы, часть которых сейчас оказались недоступными.

Другие эксперты по кибербезопасности затруднились оценить количество утечек в сегменте доставки еды. По словам эксперта по кибербезопасности «Лаборатории Касперского» Дмитрия Галова, если на специализированном форуме появилась информация о продаже базы данных, она не обязательно новая. «Она может быть скомпилированной из других баз или вообще не содержать никакой информации. И даже если базы действительно утекли, информация о пользователях может пересекаться», — рассуждает он. Возможный рост случаев утечек, по его мнению, может быть связан с ростом числа сервисов доставки еды на фоне пандемии, а также с тем, что созданием подобных компаний часто занимаются небольшие организации, у которых не всегда хватает ресурсов на поддержание высокого уровня безопасности при сборе и хранении данных.

Руководитель направлений комплаенса и аудита управления информационной безопасности Softline Илья Тихонов отметил, что в компании наблюдают регулярные утечки в отрасли доставки еды, потому что такие сервисы собирают больше всего данных. Такие сервисы не относятся к категории критической инфраструктуры, финансовой или медицинской деятельности, и закон не обязывает их защищать сведения сильнее, чем в других отраслях. При этом базы данных сервисов доставки намного больше и имеют разветвленную структуру: внутри много пользователей, отделений, пунктов выдачи и т.д., то есть доступ к ним есть у многих лиц. «Подобные ресурсы привлекают злоумышленников тем, что объем персональных данных, которые оставляют их пользователи, достаточно велик (Ф.И.О., телефон, адрес электронной почты, адрес проживания, иногда платежные данные), — отметил представитель Softline. — Такая совокупность сведений имеет немалую ценность и может быть использована в самых разных противоправных сценариях».

Обычным людям предотвратить утечку крайне сложно — чтобы доставили заказ, придется оставить актуальный телефон и адрес в любом случае, напомнил руководитель аналитического центра компании Zecurion Владимир Ульянов. После этого пользователю «остается лишь надеяться, что данные будут защищены должным образом и не будут скомпрометированы».

Материалы к статье
Авторы
Теги
Екатерина Ясакова