Технологии и медиа , 12 окт, 00:00
0

Данные почти 10 млн пользователей букмекерской платформы утекли в Сеть

Из-за чувствительности данных теперь клиенты рискуют стать жертвами фишинговых атак
В даркнете оказалась выставлена на продажу база данных о почти 10 млн учетных записей букмекерской конторы и онлайн-казино Pin-Up.bet. Большая часть данных связана с Россией, и эксперты назвали их очень чувствительными

BI.ZONE, «дочка» Сбербанка, которая занимается управлением цифровыми рисками, обнаружила на теневом форуме информацию о продаже базы данных пользователей букмекерской платформы Pin-Up.bet. Жертвами утечки стали более 9,975 млн человек, из них чуть более 7,8 млн аккаунтов были зарегистрированы в России, еще 1,3 млн — в Великобритании, 600 тыс. — в Турции, остальные — в Бразилии, США, Германии и Азербайджане.

Владелец базы готов продать ее за $10 тыс., оплата принимается в криптовалюте. За эти деньги он обещает предоставить покупателю данные об электронной почте пользователей, дате рождения, номере телефона, финансовую информацию, адрес, пол, любимую игру, в которой сделано наибольшее количество ставок, и пр.

«Автор объявления заявляет, что продаваемая база актуальна на конец 2020 года. Для предотвращения вероятных последствий мы рекомендуем пользователям сменить пароли и настроить двухфакторную аутентификацию, если это возможно», — сообщил директор блока экспертных сервисов BI.ZONE Евгений Волошин. В сэмплах (образцах данных отдельных пользователей) указаны персональные данные, в числе которых город, адрес, телефон и др., убедился корреспондент РБК.

Факт наличия такой базы в продаже с 5 октября РБК подтвердили руководитель группы исследования публичных утечек Group-IB Олег Дёров и основатель сервиса анализа утечек данных DLBI Ашот Оганесян.

Что такое Pin-Up.bet

Pin-Up.bet позволяет совершать ставки на спорт и играть в онлайн-казино. В России деятельность онлайн-казино запрещена, и международная версия сайта заблокирована по решению Федеральной налоговой службы (ФНС), однако пользователям доступны его зеркала. Кроме того, в России работает сайт Pin-Up.ru, который принимает только ставки на спорт, не предоставляя возможность играть в онлайн-казино. Причем владелец доменного имени pin-up.ru ООО «Уильям Хилл» указан в реестре организаций по проведению азартных игр в букмекерских конторах или тотализаторах ФНС.

«Pin-Up.bet является нашим партнером, но прямого отношения к этой компании мы не имеем, — сообщил консультант Pin-Up.ru в ответ на запрос РБК. — Разница в том, что Pin-Up.ru является лицензированной букмекерской компанией, работаем согласно российскому законодательству, у нас предоставляются только ставки на спортивные события». Он также отметил, что у них нет информации по Pin-Up.bet.

В отличие от нелегальных легальные букмекеры платят налоги, выполняют требование по максимальному размеру вознаграждения, взимаемого организатором азартных игр в тотализаторе с участников (не выше 30%) и т.д., пояснил управляющий партнер юридической компании AVG Legal Алексей Гавришев.

Насколько крупная утечка

«Случаи, когда в сеть утекают данные букмекерских платформ, происходят довольно редко. Я бы сказал, что это крупный слив. Скорее всего, взломали сервер. Слить могли через какую-то уязвимость

вроде SQLi (один из распространенных способов взлома сайтов и программ, работающих с базами данных)», — отмечает Оганесян. В то же время он сомневается, что кто-то купит базу за указанную продавцом цену, назвав ее слишком высокой.

Олег Дёров назвал утечку достаточно крупной, однако не рекордной ни для мира, ни для России. Например, в 2012–2014 годах произошли массовые утечки «ВКонтакте» и «Рамблера», каждая из которых содержала данные о более чем 90 млн пользователях. В сентябре 2021 года команда Group-IB обнаружила около 120 опубликованных (не на продажу) баз данных, семь из которых были крупнее, чем утечка Pin-Up.bet. При этом одна из самых массовых утечек данных букмекерских платформ произошла в январе 2019 года, когда из-за отсутствия пароля на публичном сервере ElasticSearch утекли данные группы онлайн-казино Mountberg Limited (включает kahunacasino.com, azur-casino.com, easybet.com, viproomcasino.net и др.), напомнил Ашот Оганесян. База содержала информацию о более чем 108 млн ставок, выигрышей, депозитов и выводов денег. Кроме того, утекли имена, домашние адреса, номера телефонов, адреса электронной почты, даты рождения, балансы аккаунтов, IP-адреса, списки игр, в которые играли игроки и т.п.

Чаще всего базы данных, выставляемые на продажу в даркнете, попадают к злоумышленникам в результате успешных атак на инфраструктуру организации либо посредством кражи с корпоративных серверов с незакрытым доступом в интернет, либо, что реже, в результате слива данных внутренним сотрудником, рассказал эксперт Центра продуктов Dozor компании «Ростелеком-Солар» Алексей Кубарев. Он также отметил, что, как правило, при регистрации пользователи различных букмекерских сервисов и онлайн-казино предоставляют достаточно полный набор своих персональных данных, включая адрес проживания, мобильный телефон, e-mail и другую чувствительную информацию.

«В самом факте утечки нет ничего удивительного. Букмекерский сайт всегда привлекает злоумышленников, ведь он напрямую связан с финансовыми операциями. Исходя из предоставленной информации, утечка видится весьма крупной, однако надо понимать, что 10 млн учетных записей — это не 10 млн уникальных пользователей. На подобном сайте всегда будет много «мертвых» учеток, а также масса учетных записей, принадлежащих одним и тем же людям, пусть даже это и противоречит пользовательскому соглашению», — отметил руководитель отдела анализа цифровых угроз компании «Инфосекьюрити» (входит в группу Softline) Александр Вураско, оговорившись, что компания не располагает сведениями об утечке.

Чем инцидент грозит пользователям

Олег Дёров говорит, что хотя конкретно в этой утечке пароли к аккаунтам хранились не в открытом виде, но даже без паролей утечка представляет угрозу для пользователей. «Огромное количество электронных адресов и телефонов позволяет злоумышленникам проводить массовые спам-рассылки. А со знанием дополнительных данных из этой утечки (имен, адресов, дней рождения, данных об аккаунте и т.д.) злоумышленники могут провести целевые фишинг- и вишинг-атаки (киберпреступления, направленные на кражу личной информации по телефону)», — отметил он. Подобная утечка может обернуться для скомпрометированных пользователей либо попытками скама от мошенников, когда злоумышленник сначала втирается к пользователю в доверие, а потом вынуждает раскрыть данные и отдать деньги, либо спамом от других букмекеров, согласен Ашот Оганесян.

При этом Александр Вураско обратил внимание на то, что политика обработки персональных данных Pin-Up.bet допускает весьма расплывчатые формулировки, в частности их передачу третьим лицам. Согласно одному из пунктов пользовательского соглашения, компания не несет ответственности за любой причиненный ущерб или убытки, включая, но не ограничиваясь, потерей данных, дохода, престижа, репутации, а также за любые потери, которые она не может предусмотреть. В том же соглашении указано, что все споры регулируются законодательством Кипра.

Автор
Екатерина Ясакова