«Алло, мы вас взломали!»: рекомендации «Информзащиты» по противодействию ложной атаке на аккаунты пользователей

Издание: CRN, 27 июля 2018 г.

Спикер: компания «Информзащита»

В июле 2018 года в сети Интернет зафиксированы случаи ложных атак на личные кабинеты пользователей и их персональные данные. Эксперты «Информзащиты» предупреждают: не доверяйте информации о том, что в вашу инфраструктуру проникли, пока не убедились в этом достоверно или не получили подтверждение от профессионала по информационной безопасности.

Обычно ситуация выглядит следующим образом: злоумышленник сообщает, что после успешной атаки смог получить доступ к базе данных с аккаунтами и персональными данными ваших клиентов. В подтверждение своих слов злоумышленник демонстрирует несколько сотен записей из якобы попавшей в его руки базы с некоторой чувствительной информацией типа данных о количестве бонусных баллов, последних действиях этих пользователей и т.п. Подобному обращению может реально предшествовать атака, связанная с перебором паролей к личным кабинетам пользователей. Проверка покажет, что представленные данные актуальны, и это вызовет доверие к словам злоумышленника.

Цель такого поведения — получить вознаграждение за молчание и сокрытие информации о якобы произошедшей утечке. В случае отказа злоумышленник угрожает опубликовать конфиденциальные данные клиентов.

На самом деле, заявляемая информация об утечке может оказаться блефом. Суть в том, что хакерам порой действительно удается взломать и украсть учетные данные пользователей к некоторым интернет-магазинам, форумам, социальным сетям, игровым сайтам. Причем от утечек не застрахованы и крупные сетевые компании. Так, например, в 2016 году произошла утечка более 25 млн учётных данных пользователей Mail.ru. В 2014 году зафиксирована утечка учётных данных пользователей «Яндекс.Почты» (1,26 млн паролей) и пользователей Gmail (5 млн паролей). Учетные данные пользователей могут попадать в руки злоумышленников и после проведения удачной вирусной или фишинговой атаки.

Данные об учетных записях пользователей являются ходовым товаром на черном рынке, но иногда они публикуются и в открытом доступе. На текущий момент крупнейшей базой данных украденных паролей является BreachCompilation, опубликованной в декабре 2017 года исследователями безопасности из компании 4iQ. База содержит 1,4 млрд учетных данных и включает в себя данные предыдущих «сливов», таких как Anti Public Combo List и Exploit.in.

В рассматриваемом случае, злоумышленник пользуется тем, что многие люди, дабы облегчить себе жизнь, используют один и тот же пароль на многих интернет-ресурсах. Перебор нескольких сотен тысяч таких взломанных учеток на любом сайте вполне может дать несколько сотен доступов к реальным аккаунтам пользователей. Именно эти данные злоумышленник и представит для проверки.

Эксперты «Информзащиты» рекомендуют в такой непростой ситуации сохранять хладнокровие и не торопиться удовлетворять требования вымогателя. Оперативное подключение специалистов позволит проверить информацию о потенциальном взломе, поможет выстроить тактику общения с злоумышленником и даст возможность привлечь вымогателя к ответственности.

Для того, чтобы не стать жертвой подобной атаки, аналитики «Информзащиты» рекомендуют применять меры защиты, которые затруднят злоумышленникам перебор паролей к учетным записям пользователей, а именно:

- защита веб-сайтов от интернет-ботов методом reCAPTCHA;
- двухфакторная аутентификация пользователей при доступе в личные кабинеты (смс-подтверждение и пр.)
- смена паролей на периодической основе и в случае подозрения их компрометации.

Безопасность — это не только настроенные средства защиты, но и правильные решения, принимаемые в необычных или критичных ситуациях.

Подробнее: https://www.crn.ru/news/detail.php?ID=128052