Криптобиржа подвела очередного клиента и продолжает игнорировать проблему.

В Китае хакер использовал вредоносное расширение Google Chrome – браузер, который разрабатывается на основе свободного проекта Chromium. Для отображения web-страниц браузер использует движок WebKit.

 Первая публичная бета-версия Google Chrome была представлена 2 сентября 2008 года, а первая стабильная версия – 11 декабря 2011 года. Изначально Chrome выпускался только под Microsoft Windows. Позже браузер был выпущен для Linux, macOS и мобильных платформ.

 Браузер Chrome нацелен на повышения уровня безопасности пользователей за счет максимально высокой скорости работы, а также минимально допустимого функционала. Все дополнительные функции в браузер внедряются за счёт сторонних расширений." data-html="true" data-original-title="Chrome" >Chrome, чтобы получить доступ к аккаунту пользователя на Binance – это одна из крупнейших в мире криптовалютных бирж, основанная в 2017 году Чанпэном Чжао. Биржа предоставляет платформу для торговли различными криптовалютами, такими как Bitcoin, Ethereum, и многими другими. Binance известна своим широким ассортиментом торговых пар, низкими комиссиями и высокой скоростью обработки транзакций. Помимо обычной торговли, Binance предлагает пользователям дополнительные услуги, такие как стейкинг, фьючерсные контракты, кредитование, а также запуск собственных токенов через платформу Binance Launchpad." data-html="true" data-original-title="Binance" >Binance и незаметно украсть криптовалюту на сумму в один миллион долларов. Свою историю пострадавший под ником Nakamao рассказал на платформе X.

Хакер использовал расширение под названием Aggr для перехвата сессионных файлов куки Binance, что позволило ему авторизоваться без ввода пароля и двухфакторной аутентификации. Nakamao заподозрил неладное, когда зашел на платформу, чтобы проверить курс биткоина, и заметил подозрительную торговую активность в своем аккаунте.

Особенность метода хакера заключалась в следующем: он продавал переоцененные токены с контролируемого им аккаунта, покупая их на средства Nakamao, а затем продавал эти токены по рыночной цене, получая прибыль. Таким образом его махинации не вызывали никаких подозрений у системы безопасности сервиса.

После обнаружения кражи Nakamao обратился в службу поддержки Binance, но необходимой помощи не получил. Тогда он решил попросить помощи у независимых консультантов, которые и выяснили, что злоумышленник использовал расширение Aggr, установленное по рекомендации криптовалютного инфлюенсера. В ходе расследования также стало известно, что Binance уже знала о существовании этого

вредоноса, так как ранее он использовался для взлома другого аккаунта на платформе.

Nakamao выразил недовольство системой безопасности сервиса. Особенно его возмущает тот факт, что после первого инцидента с участием того же хакера компания не предприняла должных мер.

«Если бы хакер просто вывел средства, я бы смирился, но его манипуляции с перекрестной торговлей и последующие действия Binance неприемлемы. Тем более, что Binance уже давно следит за действиями преступника и изучает расширение, но это ни к чему не приводит», — поделился Nakamao.

Когда пост Nakamao стал распространяться по сети, Binance также опубликовала заявление в X . Компания подчеркнула, что саму платформу никто не взламывал, и призвала пользователей избегать установки подозрительных браузерных расширений: «Несмотря на то, что платформа Binance не была взломана, мы хотим, чтобы сообщество оставалось бдительным. Избегайте установки браузерных расширений, так как они могут украсть ваши данные и поставить под угрозу безопасность вашего аккаунта».

Недавние исследования показали, что создание вредоносных приложений для Chrome, которые крадут файлы куки пользователей – довольно несложный процесс. Даже не будучи программистом, код для такой программы можно написать, например, с помощью ChatGPT.