

Фатальная 0day-уязвимость была устранена всего за 47 минут, но было уже поздно.

Популярная криптобиржа Kraken — это крупная русскоязычная даркнет-площадка, появившаяся в 2022 году после закрытия Hydra. Однако важно помнить, что использование даркнета связано с определенными рисками, такими как мошенничество, утечка данных и правовые последствия. Стоит отметить, что:

- Деятельность Kraken является незаконной: торговля наркотиками, оружием и другими запрещенными товарами является уголовно наказуемым деянием.
- Использование Kraken может быть небезопасным: существует риск мошенничества, утечки данных и других проблем.
- Даркнет часто используется для криминальной деятельности: Kraken может быть использован для совершения преступлений, таких как отмывание денег, торговля людьми и киберпреступность.

Kraken сообщила о краже \$3 миллионов из-за критической уязвимости нулевого дня, которую обнаружил неназванный исследователь безопасности и сам же «по-тихому» ей воспользовался. Ник Перкоко, главный директор по безопасности Kraken, рассказал, что уязвимость позволила недобросовестному исследователю искусственно увеличивать баланс на платформе.

Компания быстро выявила мошенническую активность, позволявшую инициировать депозит и получать средства без его полного завершения. Несмотря на то, что активы клиентов не пострадали, проблема могла позволить злоумышленнику создавать новые активы на своих счетах.

Как сообщается, проблема возникла из-за недавнего изменения интерфейса, который позволял клиентам использовать внесённые средства до их полной очистки. Расследование показало, что уязвимостью воспользовались трое пользователей, включая горе-исследователя. А устранена она была за рекордные 47 минут.

Перкоко уточнил, что вышеуказанный исследователь первым обнаружил баг и использовал его для зачисления \$4 на свой счёт. Он мог бы сообщить о нём в рамках программы вознаграждений и получить солидную выплату, однако решил поделиться находкой с двумя другими лицами, которые сгенерировали гораздо большие суммы и вывели с биржи почти 3 миллиона долларов.

Когда Kraken попросила вернуть украденные средства, злоумышленники потребовали связаться с их командой для уплаты выкупа. Компания расценила данный шаг как вымогательство, поэтому рассматривает инцидент как уголовное дело и сотрудничает с

правоохранительными органами.

Перкоко подчеркнул, что исследователи безопасности должны следовать правилам программы вознаграждений, иначе их действия становятся незаконными и подлежат справедливому наказанию в рамках законодательства.