Управление уязвимостями в криптокошельках

Александр Подобных, *глава департамента расследований BitOK, руководитель Санкт-Петербургского РО АРСИБ, руководитель Комитета по безопасности цифровых активов и противодействию мошенничеству, судебный эксперт*

Криптовалюта не лежит на кошельках, это всего лишь способ хранения закрытого (секретного) ключа. Примерно как на пластиковой банковской карте нет самих денег, она лишь открывает доступ к банковскому счету. Кошельки — это программные или аппаратные средства, которые подвержены уязвимостям. Разберемся, в чем их особенность и какими методами обеспечивается информационная безопасность в этой области.

Проблемы и угрозы

Криптовалютные кошельки во всем их многообразии можно поделить на две большие категории: к холодным относят аппаратные, к которым есть физический доступ, а к горячим – браузерные или мобильные приложения.

Холодные кошельки не подключаются к Интернету и считаются самыми безопасными – это бумажные кошельки, флешки и т.п. Их нужно подключать к компьютеру или телефону для совершения транзакций.

Важно отметить, что при использовании холодных криптокошельков за сохранность закрытых ключей и средств, к которым они предоставляют доступ, несет сам владелец, а при использовании горячих ответственность ложится на оператора сервиса (кастодиана или депозитарий).

Основные проблемы и угрозы, с которыми сталкиваются пользователи криптовалютных кошельков, включают в себя следующие.

1. Взломы и кибератаки. Криптовалютные кошельки могут стать целью злоумышленников, которые стараются получить доступ к частным ключам и совершить кражу средств.

2. Фишинг. Злоумышленники могут создавать поддельные веб-сайты и электронные письма, имитирующие официальные криптовалютные сервисы, на которых пользователи вводят свои аутентификационные данные и теряют доступ к средствам.

3. Потеря доступа. В случае утери пароля, закрытого ключа или резервной фразы пользователи могут лишиться доступа к своим средствам без возможности их восстановления. К утере можно отнести также и невозможность их вспомнить.

4. Социальная инженерия. Атаки могут быть направлены не только на технические слабые места, но и на слабые места в поведении пользователей, которые подвергаются обману с целью раскрытия их конфиденциальных данных.

5. Влияние человеческого фактора. Ошибки в управлении кошельком, неверное сохранение частного ключа или резервной фразы также могут привести к потере средств.

6. В последние годы для российских пользователей высокие риски несут санкции, реализуемые площадками по требованию иностранных регуляторов (OFAC, SEC, FCA). При этом одни биржи просто блокируют кошельки (так поступили большинство площадок), другие же дают время на вывод средств (как было с Binance в 2023 г.).

7. Растет также количество взломов, связанных с инсайдерами в самих проектах. Они сливают информацию о кошельках, платформах, протоколах взаимодействия.

8. Многих разработчиков в последнее время интересует защита от квантовых компьютеров, в частности защита от перебора приватных ключей. Возможно, угроза со стороны квантовых компьютеров преувеличена, однако она все же существует, и многое зависит от того, какие шаги предпримут блокчейн-разработчики до того момента, когда эта угроза станет более реальной. К примеру, разработчики Ethereum ведут разработку устойчивых к квантовым атакам методов криптографии, таких как подписи Winternitz и технология с нулевым разглашением STARK.

Примеры уязвимостей и их эксплуатации

В феврале 2018 г. сообщество отметило несколько новостных статей, в которых утверждалось, что Национальный институт стандартов и технологий (NIST) активно расследует уязвимость 2018 г. в приложении iOS Trust Wallet, которая была оперативно исправлена в том же году. Разработчики заверили пользователей в том, что их средства в безопасности, а кошельки безопасны для использования.

В августе 2022 г. произошла крупная кража токенов из кошелька Solana, которая была вызвана уязвимостью централизованного сервера Sentry. Исследователи обнаружили две новых технологии сбора данных из Solana, которые могут выполнять атаки с перестановкой битов.

В конце ноября 2023 г. 1,5 млн биткойнов оказались под угрозой хищения из-за уязвимости Randstorm, которая позволяет восстанавливать пароли и получать несанкционированный доступ к множеству кошельков на разных блокчейн-платформах. Уязвимость связана с использованием BitcoinJS – открытой JavaScript-библиотеки для разработки криптовалютных кошельков в браузере. Проблема заключалась в недостатке энтропии, которую можно использовать для проведения брутфорс-атак и восстановления сгенерированных приватных ключей кошельков, причем уязвимости в базовых библиотеках, используемых в открытых проектах, могут иметь каскадные риски для всей цепочки поставок.

В декабре 2023 г., "надписи" на биткойнах были добавлены в Национальную базу данных уязвимостей США (NVD) и отмечены как угроза кибербезопасности. Это было сделано для привлечения внимания к недостаткам безопасности, которые были допущены при разработке