чаются недостаточным уровнем безопасности, атака Double-Spending может быть еще более успешной, если атакующие смогут внести изменения в исходный код блокчейна или в майнинг-процесс.

Double-Spending остается одним из ключевых вызовов для блокчейн-систем, и исследователи и разработчики продолжают искать эффективные методы борьбы с этой угрозой. Для предотвращения атак Double-Spending блокчейн-системы используют различные защитные меры и протоколы. Методы подтверждения транзакций, такие как Proof-of-Work и Proof-of-Stake, помогают уменьшить вероятность успешной атаки. Многие блокчейны также используют механизмы консенсуса и проверки подлинности для обеспечения безопасности транзакций.

Атаки с повторным входом

Если кроссчейн-мост включает смарт-контракты, злоумышленник может попытаться многократно вызывать функции смарт-контракта перед завершением предыдущего вызова, этот сценарий называют Reentrancy. Обычно он используется для многократного списания средств, изменения состояния контракта или других манипуляций.

Кроме того, кроссчейны подвержены и обычным атакам DoS и DDoS.

Для снижения рисков и защиты от этих атак разработчики применяют различные техники: улучшенные смарт-контракты, криптографические методы и др. Важным элементом является тщательное тестирование и аудит безопасности при создании кроссчейн-мостов.

В качестве системы защиты используются также многоподписные схемы (Multisignature, Multisig) – это системы криптографических схем, позволяющие нескольким пользователям совместно управлять средствами или совершать транзакции. Чтобы не зависеть от одного ключа или одного пользователя, многоподписные схемы предполагают подписи от нескольких ключей для авторизации и выполнения определенных действий.

Атаки на сайдчейны

Угрозой для сайдчейнов являются атаки 51%, особенно если этому типу атак подвержены используемые в сети консенсусные алгоритмы. Злоумышленник, контролируя большую часть вычислительной мощности сети, может манипулировать транзакциями, отклонять блоки и влиять на общий порядок событий в сайдчейне.

Смарт-контракты в сайдчейнах подвержены рекурсивным атакам, переполнению стека и другим видам эксплойтов. Защита от таких атак требует внимательного аудита смарт-контрактов и использования безопасных программных паттернов.

И, конечно же, наиболее опасны комбинированные атаки, когда используются сразу несколько методов. Например, злоумышленники могут сочетать атаку 51% с эксплойтом уязвимости в смарт-контрактах для достижения максимального воздействия.

Известные успешные атаки

В феврале 2022 г. стало известно об атаке на кроссчейн-мост Wormhole, который осуществлял обмен активами между сетью Solana и другими блокчейнами, в том числе со сверхпопулярным Ethereum. Злоумышленники обнаружили метод эмиссии необеспеченных токенов, которые они обменяли на реальные криптовалюты. В общей сложности экосистема Solana подверглась четырем атакам, а общий ущерб от них составил $397 млн.

В конце марта 2022 г. атака на сайдчейн Ronin, специально созданный для улучшения масштабируемости и снижения комиссий для пользователей игры Axie Infinit. Благодаря вредоносному ПО в PDF-документе с предложением о работе от несуществующей компании, загруженном одним из сотрудников из электронного письма, злоумышленники успешно осуществили атаку и вывели криптовалютные активы на $625 млн.

Заключение

Технологии сайдчейнов и кроссчейнов используются очень активно, они являются шлюзами обмена средствами и ценностями между разными сегментами рынка криптовалют.

Становится понятно, почему хакеры всех мастей обратили свой взор на кроссчейн-мосты и сопутствующие протоколы. С ними были связаны самые крупные кражи за 2022 г., согласно отчету Chainalysis: в общей сложности ущерб составил сумму, эквивалентную $3 млрд.

Примечательно, что эксперты прогнозируют по итогам 2023 г. в разы больший ущерб: уже были зафиксированы крупные атаки на популярные площадки и за несколько месяцев текущего года объем похищенных активов уже сравнялся с показателями 2022 г.

Ведущие аналитические платформы и их специалисты не дремлют, ищут похищенные средства, мошенников, блокируют их на криптовалютных биржах и в протоколах. Такие платформы осуществляют анализ большого объема данных о транзакциях, кластеризацию адресов криптокошельков, ранжирование рисков, визуализацию данных для упрощения анализа.

Участниками рынка очень востребованы новые подходы к Data Science с углублением исследования атрибутов, кроме того, на рынке не хватает аналитиков. Доступны корпоративные решения, есть платформы Open Source, поддерживаемые сообществом экспертов,

для анализа транзакций между блокчейнами. Разработан специализированный инструментарий для блокчейн-криминалистики между сайдчейнами и кроссчейнами.

Для повышения защищенности сайдчейнов и кроссчейн-мостов необходимо повышать прозрачность и стандартизацию, делать аудиты на соответствие отраслевым стандартам и пентесты, обязательно и внедрение безопасной разработки SDLC, в том числе и для повышения качества разработки смарт-контрактов.

Возможно, сейчас блокчейны и кажутся уделом гиков, а их проблемы выглядят локальными. Но блокчейн активно проникает в разнообразные отрасли экономики и приживается там в виде инновационных бизнес-приложений. Все риски, присущие технологии, становятся актуальными не только для криптовалютных организаций, но и для традиционных сфер. Поэтому готовность к защите критичных процессов на базе блокчейнов через три-пять лет должна закладываться уже сегодня. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru