LinkingLion: операция по деанонимизации биткоина

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

Анонимность является одной из ключевых особенностей и привлекательных характеристик биткоина, которая способствует его популярности среди пользователей, и особенно среди тех, кто ценит конфиденциальность своих финансовых операций. Однако в начале 2023 г. исследователи обнаружили серьезную угрозу анонимности участников сети биткоина со стороны объекта, названного LinkingLion.

Что такое мемпул?

Под мемпулом (Mempool) в криптосфере понимается хранилище неподтвержденных транзакций в сети блокчейна. Когда пользователь отправляет транзакцию с использованием криптовалюты, она сначала попадает в мемпул, очередь транзакций, которые еще не были включены в блок и не получили подтверждения майнерами или участниками сети.

Участники сети могут просматривать мемпул и выбирать транзакции для включения в новый блок на основе различных факторов, таких как размер комиссии, приоритетность транзакции и других предпочтений.

Размер мемпула может колебаться в зависимости от активности сети и объема отправляемых транзакций. В периоды высокой активности сети мемпул может становиться полностью заполненным, что приводит к увеличению времени подтверждения транзакций или повышению комиссий для более быстрого включения.

Мемпул играет важную роль в обеспечении функционирования блокчейна и подтверждения транзакций. Отслеживание состояния мемпула может быть полезным для пользователей, которые хотят оптимизировать время подтверждения своих транзакций или выбрать подходящую комиссию для быстрого включения в блок.

Участники сети могут просматривать мемпул и выбирать транзакции для включения в новый блок на основе различных факторов, таких как размер комиссии, приоритетность транзакции и других предпочтений.

Что же случилось?

В марте 2023 г. эксперт под псевдонимом b10c опубликовал исследование под названием LinkingLion[1], посвященное анализу поведения фальшивых узлов. Он обнаружил в блокчейн-сетях "Биткоин" и "Монеро" некий объект, собирающий информацию о транзакциях при их попадании в мемпул.

Конечно, это может быть проявлением работы некоей исследовательской компании, занимающейся анализом блокчейна для улучшения своих продуктов. Но автор предполагает, что это кампания по деанонимизации пользователей.

Исследуемый объект ведет себя так: открывает соединения со многими биткоин-узлами, используя четыре диапазона IP-адресов, и прослушивает анонсированные транзакции, потенциально соотнося новые широковещательные транзакции с IP-адресами узлов. Используемыми диапазонами пользуются четыре компании: Fork Networking, Castle VPN, Linama, Data Canopy, а все диапазоны относятся к провайдеру LionLink Networks. Поэтому автор для созвучия назвал исследуемый объект LinkingLion, а затем высказал гипотезу, что LinkingLion пытается связать все выявленные транзакции с IP-адресами, то есть речь идет о попытке деанонимизации участников.

Не ясно, управляется ли описанный в исследовании объект LinkingLion единым человеком, группой лиц или организацией. Но соединения используют общие шаблоны для различных диапазонов IP-адресов. Кроме того, все диапазоны используют одни и те же поддельные данные о пользовательских агентах, то есть, скорее всего, используется одно программное обеспечение. Конечно, это лишь косвенное подтверждение того, что за подключениями стоит одна организация.

Далее исследователь обратил внимание на то, что один из диапазонов IP-адресов принадлежит компании под названием Castle VPN, что наводит на мысль, что LinkingLion открывает соединения через VPN-сервис. Другие диапазоны IP-адресов также можно было бы использовать в качестве конечных точек VPN, что объяснило бы, почему несколько конфигураций программного обеспечения используют одни и те же адреса. Однако и эта теория пока остается неподтвержденной.

Какая информация доступна LinkingLion?

Информация, которую получает LinkingLion, может быть вычленена из метаданных, сведений по инвентаризации и адресам. Вообще, любое соединение может получить метаданные узла, с которым оно устанавливается, включая:

- информацию о доступности узла;
- версию используемого программного обеспечения;
- параметры блокчейн-транзакций, предпочитаемые узлом;

[1] *https://b10c.me/observations/06-linkinglion/*