● список услуг, предоставляемых узлом.

Временная информация, то есть когда узел объявляет о своем присутствии или обновлении инвентарных сведений, особенно актуальна для последующего анализа.

Поскольку LinkingLion подключается ко многим прослушивающимся узлам, он может использовать набор получаемых сведений для привязки широковещательных транзакций к IP-адресам, а значит, потенциально и к пользователям.

Около 2% подключений со стороны объекта LinkingLion также просят узел отправить им адреса других узлов сети. Объект, вероятно, использует их для поиска новых адресатов для подключения и увеличения доли охваченных узлов, а также может попытаться распознать топологию сети, отслеживая ретрансляцию транзакций.

Остается загадкой, зачем LinkingLion открывает несколько кратковременных подключений к одному узлу из нескольких диапазонов IP-адресов. Всю информацию можно было бы извлечь и без многократного открытия и закрытия соединений, не привлекая внимания исследователей. Впрочем, это вполне можно списать на ошибки в логике работы самого LinkingLion.

Автор исследования впервые лично наблюдал действия LinkingLion летом 2022 г., однако объект был активен дольше. Отрывочные сведения, ретроспективно обнаруживаемые в некоторых отчетах в Интернете, свидетельствуют, что операции LinkingLion проводились как минимум с начала 2018 г.

Кто стоит за LinkingLion?

Большинство P2P-аномалий, происходящих с открытой сетью биткоина, исходят от частных лиц или компаний, преследующих либо академические цели, либо корыстные (например, продажа собранных данных другим компаниям и правоохранительным органам).

В случае с LinkingLion академический интерес кажется маловероятным: вряд ли обычный исследователь будет финансировать такую масштабную операцию в течение нескольких лет, ведь диапазоны IP-адресов и серверы стоят немалых денег. К тому же академические эксперименты обычно более локализованы по времени, да и опубликованных по итогам статей пока найти не удалось.

Коммерческим компаниям есть смысл платить за инфраструктуру, если они смогут выгодно продать собранные данные или улучшить с их помощью свой продукт в сфере блокчейна. Так что вариант, когда за LinkingLion стоит некая организация, выглядит более правдоподобным.

Что же делать?

Первоочередной мерой противодействия может стать ручная блокировка диапазонов IP-адресов, используемых LinkingLion, то есть запрет для них входящих подключений к узлам.

Однако это действие не решает проблему полностью, ведь LinkingLion может легко переключиться на новые диапазоны IP-адресов. Основная опасность заключается в том, что по итогам сбора информации со стороны LinkingLion может быть установлена высоковероятная связь транзакций и IP-адресов. Чтобы этого не допустить, потребуются изменения в логике первоначальной трансляции и ретрансляции транзакций в сети биткоина и в ядре Bitcoin Core.

Технологическим решением может стать технология Dandelion, например Dandelion++ или какая-либо из ее модификаций.

Dandelion (англ., одуванчик) – это протокол передачи транзакций в сети блокчейна с целью повышения анонимности и защиты приватности пользователей. Он был разработан в 2017 г. для биткоин-сети, хотя может быть реализован и в других блокчейнах.

Основная идея Dandelion заключается в том, чтобы затруднить определение источника транзакции в сети блокчейна, что может повысить уровень анонимности для отправителей транзакций. По умолчанию, когда транзакция создается, она отправляется на первый узел в сети и начинает свой путь к остальным узлам через прямой маршрут. Это как раз и может делать возможным отслеживание источника транзакции.

Протокол Dandelion модифицирует этот процесс: вместо прямой передачи транзакция отправляется на случайно выбранный узел, который называется "стебель" (Stem Phase). Этот узел удерживает транзакцию на некоторое время и затем, после искусственной временной задержки, передает ее дальше группой узлов вместе, образуя так называемые "колосья" (Fluff Phase). Таким образом, точное место отправителя транзакции становится труднее обнаружить.

Dandelion++ используется в блокчейн-сети Monero с 2020 г. Попытка аналогичного внедрения в Bitcoin Core так и не увенчалась успехом, в первую очередь из-за сложности и проблем с DoS.

Заключение

Гипотезы и выводы, приведенные в исследовании, выглядят вполне обоснованными как с технической точки зрения, так и с точки зрения общей картины развития криптосферы. За последние пять лет на рынке анализа блокчейн-транзакций появилось много новых игроков, в том числе и очень крупных. В СМИ то и дело появляются новости об очередном выигранном госконтракте или получении дополнительных инвестиций, исчисляемых уже десятками и сотнями миллионов долларов. Причем если анализом биткоина, эфириума и их форков занимаются многие компании, то, к примеру, на деанонимизацию и анализ технологии Monero выделялись прямые исследовательские гранты на сотни миллионов долларов.

Зная также о государственно-частном партнерстве американской компании Chainalysis с ФБР и другими ведомствами, а также доступных сведениях о существовании модуля интеграции с системой аналитики Palantir (используют спецслужбы, инвестиционные банки, хедж-фонды), можно предположить, что такой глобальный сбор IP-адресов необходим, как вариант, для массового выявления субъектов с высоким уровнем риска (по AML/CFT) и преступников.

Недавно, в 2023 г., один из игроков в блокчейн-аналитике анонсировал применение ИИ для сквозной блокчейн-аналитики между различными блокчейнами и токенами. По-видимому, похожие работы уже ведутся в нашей стране. А значит, не исключено появление новых исследовательских объектов, подобных LinkingLion. ●

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

В случае с LinkingLion академический интерес кажется маловероятным: вряд ли обычный исследователь будет финансировать такую масштабную операцию в течение нескольких лет, ведь диапазоны IP-адресов и серверы стоят немалых денег.

Первоочередной мерой противодействия может стать ручная блокировка диапазонов IP-адресов, используемых LinkingLion, то есть запрет для них входящих подключений к узлам.

Основная идея Dandelion заключается в том, чтобы затруднить определение источника транзакции в сети блокчейна, что может повысить уровень анонимности для отправителей транзакций.