Секция «LegalTech. Цифровая криминалистика»

Особенности механизма следообразования при расследовании преступлений, совершенных с использованием криптовалют в случае применения дополнительных способов анонимизации

Научный руководитель – Мещеряков Владимир Алексеевич

Маркарян Эльвира Сергеевна
Выпускник (магистр)
Воронежский государственный университет, Воронеж, Россия
E-mail: seledkva@mail.ru

Опытные пользователи, которые хоть немного разбираются в особенностях функционирования криптовалют, наверняка знают, что Bitcoin далеко не анонимен. Все адреса в bitcoin- кошельке, так или иначе, могут быть привязаны к реальной личности. Например, если монеты куплены на бирже с обязательными процедурами подтверждения личности.

Необходимо обратить внимание, что пользователи криптовалют могут прибегать к дополнительным инструментам, помогающим сокрыть следы преступления. Поэтому не маловажным будет при проведение следственных действий установить факт наличия специально установленных программ, расширений в веб-браузерах, фактов открытия специализированных сайтов, указывающих на применение средств анонимизации.

Для сокрытия информации о своем месте нахождения преступники используют различные методы анонимизации своей активности в сети Интернет. В виду того, что самый легкий способ выявления отправителя транзакции - это сопоставление bitcoin-адреса или ID транзакции с IP-адресом, то анонимизация достигается за счет сокрытия реального IP-адреса преступника, по которому можно определить его точное местонахождение.

Перечисленные ниже методы различаются технологией, по которой будет происходить замена реального IP-адреса на другой.

1. VPN-серверы
2. HTTP-прокси
3. SOCKS-прокси
4. Выделенные серверы
5. Tor-сеть

Помимо указанных средств анонимизации, на помощь преступному сообществу приходит «mixing» - это процесс использования услуг третьей стороны, с целью исключения любых связей между адресом, с которого были отправлены криптовалюты, и адресом (или адресами), на которые они были отправлены. Часть сайтов-миксеров просит при регистрации ввести контактные данные, в том числе и e-mail адрес, на который в дальнейшем приходит письмо для подтверждения регистрации, соответственно проверка e-mail в последующем поможет выявить пользовался ли подозреваемый (обвиняемый) услугами миксеров. Большинство же сайтов-миксеров не требуют выполнения процедуры регистрации. В любом случае информация о транзакциях хранится на сервере миксера, информация с которого может быть получена спецслужбами, сложность в данном случае представляет только тот факт, что как правило серверы расположены на территории иностранных государств и то, что может быть применено повторное смешивание, но уже пропустив монеты через другой миксер.

Деанонимизировать пользователя миксера может помочь сопоставление всех транзакций в сети, которые отвечают определенным параметрам. К примеру, в ходе следственных действий выяснилось, что подозреваемый (обвиняемый) отправил 1 BTC на адрес bitcoin-миксера, через какое-то время на указанный им адрес получен примерно 1 BTC, который

уже никак не связан с адресом подозреваемого (обвиняемого). Но если открыть тот же blockchain.info, то можно просмотреть информацию о всех транзакциях за последнее время, которые отвечают заданным фильтрам. То есть никто не мешает найти все адреса, с которых было отправлено порядка 1 BTC, и это очень сильно сузит круг подозреваемых. А уж если знать комиссию bitcoin-миксера (как правило она составляет от 0,5 до 3%), то и вовсе можно высчитать точное количество bitcoin, которые должны получиться на выходе. Все, что остается - это найти все адреса, с которого была отправлена данная сумма (исключая адреса bitcoin-миксера, конечно). Но современные миксеры позволяют задать временную задержку и собственноручно выставленную комиссию, а также возможность указать несколько адресов приема «чистых» bitcoin, что может сильно затруднить процесс деанонимизации. Для усложнения процесса деанонимизации преступное сообщество, а также продвинутые пользователи, желающие сокрыть свои действия с криптовалютами, как правило, используют виртуальную машину с установленным на ней кошельком. Владельцы миксеров и опытные пользователи рекомендуют кошелек Electrum, но также подойдет кошелек, созданный на сайте Blockchain.info и их скрытый Tor-сервис (https://drk.li/BC), плюс взаимодействие с внешним миром только через грамотно настроенный Tor.

Стоит отметить, что многие владельцы криптовалют, а также сайты, предлагающие повысить анонимность проведения операций с криптовалютами, советуют проводить операции с помощью кошельков с высокой степенью анонимности и возможностью работать в сети TOR, а именно Electrum. Клиент работает под операционными системами Windows, Linux, Mac OS, Android. Программа установки может быть скачена с официального сайта https://electrum.org/, соответствующая операционной системе. Для ОС Windows существует и портативная версия (Portable version). Скачать программу для устройств, работающих под операционной системой Android можно через официальный магазин Google Play / http://play.google.com.

По умолчанию Electrum устанавливается на компьютеры под операционной системой:
- Windows

C:\Documents and Settings\YourUserName\Application data\ Electrum (XP)

C:\Users\YourUserName\Appdata\Roaming\ Electrum (Vista,7, 8)

Стоит учитывать, что папки "AppData" и "Application data"по умолчанию являются скрытыми.

Portable version по умолчанию устанавливается в папку загрузок. Это либо стандартная папка в директории C:\Users\ YourUserName \Downloads, либо папка, установленная по умолчанию для загрузок с браузера, либо папка в которую был отправлен файл с установочным образом программы, например electrum-2.9.2-portable.exe.

Портативная версия не отличается ничем от обычной версии, кроме возможности записать ее на любые устройства памяти и носители информации (оптические диски, внешние накопители на жестких магнитных дисках, flash-карты) и держать там кошелек вместе со всеми необходимыми файлами.
- Linux

По умолчанию Electrum устанавливается в директорию ∼/.electrum/
- Mac OS

Bitcoin устанавливается в директорию

∼/Library/Application Support/Electrum/

Рассмотрим более детально случай, если программа Electrum установлена на компьютер с операционной системой Windows. По умолчанию место установки C:\Program Files\ Electrum.

Вся информация об установленной программе Electrum будет храниться в папке

C:\Users\YourUserName\Appdata\Roaming\ Electrum

Кошелек Electrum генерирует приватные ключи с использованием технологии seed (секретная фраза, состоящая из случайно сгенерированных 12 слов-мнемонический код). Пример seed, сгенерированного при проведении исследования, «client ramp alley cheap sketch ball fury divorce injury type charge limb». Эта последовательность слов является своего рода резервной копией кошелька и может быть использована для восстановления и повторного создания всех ключей в том же или любом другом совместимом приложении кошелька. Мнемонические кодовые слова читаются и транскрибируются легче по сравнению со случайной последовательностью чисел. Seed - это очень важная последовательность английских слов, которую пользователь должен надёжно сохранить. Соответственно при проведении следственных действий необходимо обратить внимание на записи на бумажных носителях, содержащие набор несвязных английских слов. В случае, если на ПК или ином другом мобильном устройстве не будет найдено программное обеспечение, указывающее на работу с криптовалютами, то данная фраза позволит восстановить кошелёк на любой компьютере, достаточно будет просто скачать программу-кошелек. Seed также может быть сохранена в виде обычного текстового файла *.txt в произвольной директории или в виде QR-кода. В последнем случае файл сохранится как C:/Users/ YourUserName /AppData/Roaming/Electrum/qrcode.bmp.

Во многих случаях для постоянного доступа к кошельку, Electrum устанавливают на мобильные телефоны. Мобильный клиент может быть синхронизирован с десктопным клиентом, обеспечивая тем самым мультиплатформенной бумажник, установленный на нескольких устройствах, но с общим источником средств. Факт установки программы отображен в памяти устройства в папке /data/app/org.electrum.electrum-1.apk. Для просмотра места расположения системных файлов необходимы ROOT-права.

Папка, содержащая всю информацию об установленной программе находится в корневом каталоге в директории data/data/org.electrum.electrum, в данной папке находятся индивидуальные настройки приложения, библиотеки и другие файлы необходимые файлы для его работы.

Наибольший интерес вызывает содержимое папки «data». Так как именно в этой папке расположен файл кошелька. Файл кошелька default_wallet располагается в корне файловой системы устройства /data/data/org.electrum.electrum/files/data/wallets.

Так как все транзакции в сети Bitcoin прозрачны и любой желающий может проследить, на какой адрес был произведен платеж, то возникает необходимость оборвать эту цепочку, которая связывает адреса отправителя и получателя. Перемешивание bitcoin может показаться сложным для тех, кто не слишком хорошо знаком с технологией Bitcoin. Для перемешивания bitcoin требуются Tor-браузер. Скачать Tor-браузер (также известный как Onion Router) пользователь может, например, с сайта TorProject.org. Tor представляет собой отдельный браузер на базе Firefox, маскирующий настоящий IP адрес. Несмотря на то, что Tor-браузер маскирует IP-адрес и некоторые потенциально идентифицирующие пользователя браузерные характеристики, он не может считаться окончательным решением в процессе анонимизации. Использование реального имени, посещение электронной почты или авторизация в социальных медиа через Tor будут иметь точно такой же эффект деанонимизации, как при использовании обычного браузера для таких действий. Ссылки для доступа к внутресетевому домену «.onion» пользователи Tor, как правило, берут с сайта Darknetmarkets.org, на что необходимо обратить внимание при проведении следственных действий. Стоит отметить, что, начиная с релиза 0.12, клиент Bitcoin Core будет автоматически подключаться через сеть Tor, если обнаружит его установленным на ПК. Большинство других кошельков также способны соединяться через Tor, обычно эти настройки описаны в документации. Как правило, пользователи устанавливают новый

bitcoin-кошелек, который соединяется с сетью только через Tor. В этом случае прямой перевод криптовалюты из кошелька, использующегося в «чистом» интернете, на новый в сети Tor не делает владельца более анонимным. Поэтому они как правило прибегают к услугам bitcoin-миксеров. Еще одним способом анонимизации может служить использование обмена одних криптовалют на другие. Возможно еще смешивание bitcoin и altcoin, с использованием, как правило, Monero (XMR). Чтобы скрыть bitcoin, необходимо просто конвертировать их в XMR, затем переслать на новый адрес Monero, а затем переконвертировать монеты обратно в новые, анонимные bitcoin. Два сайта, хорошо подходящих для конвертации криптовалют Bitcoin и Monero друг в друга: ShapeShift.io и XMR.to. Ни один сайт не требует регистрации.

При расследовании преступлений, совершенных с использованием криптовалют следует уделять особое внимание механизму следообразования, ввиду специфики самих преступлений. В настоящей работе особое внимание уделено рассмотрению особенностям механизма следообразования, в том случае, когда пользователь прибегает к применению дополнительных способов анонимизации и обнаружению характерных следов работы «тонкого» кошелька Electrum. В виду того, что многие владельцы криптовалют, а также сайты, предлагающие повысить анонимность проведения операций с криптовалютами, советуют проводить операции с помощью кошельков с высокой степенью анонимности и возможностью работать в сети Tor. Однако это далеко не полный перечень следов, которые можно обнаружить в процессе расследования преступлений, совершенных с использованием криптовалют и требуется проведение дальнейшего более детального рассмотрения всех следообразующих объектов.

Источники и литература

1) Методы анонимности в сети. Часть 1 [Электронный ресурс] // URL: https://habrahabr.ru/post/190396/ (дата обращения 21.02.2019)

2) Методы анонимности в сети. Часть 2. Утечки данных [Электронный ресурс] // URL: https://habrahabr.ru/post/190664/ (дата обращения 16.02.2019)

3) Простое руководство по безопасному и эффективному перемешиванию биткойнов [Электронный ресурс] // URL:https://bitnovosti.com/2016/04/07/a-simple-guide-to-safely-and-effectively-mixing-bitcoins/ (дата обращения 18.03.2019)

4) Tor для Mozilla Firefox: обеспечение анонимного веб-серфинга [Электронный ресурс] // URL: http://lumpics.ru/tor-for-mozilla-firefox/ (дата обращения 15.03.2019)