нием денежных средств. В июле 2022 г. около 10% всех криптовалют, принадлежащих незаконным сервисам, были отмыты именно через миксеры.

Биткойн-криминалистика

Для биткойн-криминалистики важно, что координатор CoinJoin имеет представление о пользовательской информации, которая может позволить связать входные данные с пользователем. Это открывает возможность обнаружения значимых артефактов (свидетельств), если инфраструктура криптосервиса будет подвергнута криминалистическому анализу.

В мае 2019 г. голландская служба финансовой информации и расследований (FIOD) в тесном сотрудничестве с Европолом и властями Люксембурга конфисковала шесть серверов Bestmixer.io, контролирующих потоки Bitcoin, Bitcoin Cash и Litecoin.

Изъятие серверов злоумышленников и надлежащее восстановление информации помогают обеспечить значительную степень раскрытия анонимности этих транзакций. Если исследователям известны биткойн-адреса, принадлежащие как интересующему лицу, так и стороннему сервису микширования, они могут идентифицировать транзакции между ними.

В 2021 г. сотрудники Эдинбургского университета Нейпира опубликовали исследование[3], описывающее инструментарий и методологию для анализа сервисов смешивания биткойнов, доступ к которым был получен после судебного изъятия. Они изучили, какие реальные, общедоступные инструменты и методы раскрываются криминалистически, а также проанализировали источники артефактов, которые потребуют дальнейшего академического внимания.

Тестовая среда упомянутых кошельков была развернута на виртуальных машинах, затем использовался ряд инструментов компьютерно-технической экспертизы для исследования созданных виртуальных образов на наличие значимых артефактов. Задействованные инструменты смогли восстановить широкий спектр криминалистических свидетельств и позволили обнаружить, что сетевые активности и файлы системных журналов являются полезными источниками свидетельств для деанонимизации служб микширования.

Наиболее эффективные методы защиты от криминалистической экспертизы, используемые службами микширования, включали шифрование данных при передаче и в состоянии покоя. Obscuro микшировал в защищенном анклаве, но последующая запись этих данных на диск в зашифрованных артефактах сделала это микширование избыточным и привело к компрометации данных.

Инструменты анализа транзакций

Исследователи использовали различные наборы криминалистических инструментов, а затем по результатам их работы выполнялся поиск конкретных криминалистических артефактов. Преимущество в том, что для поиска значимых доказательств можно применять множество инструментов, предоставляющих расширенные возможности: захват файлов и потоков данных, анализ сигнатур и более глубокий синтаксический анализ конкретных приложений.

1. Autopsy, один из основных инструментов цифровой криминалистики с открытым исходным кодом, позволяющий анализировать жесткие диски, смартфоны, флеш-карты и т.д.

2. FTK Imager, программное обеспечение с открытым исходным кодом, которое было выбрано за его мощную способность монтировать и анализировать файлы образов.

3. AXIOM, платный комплексный набор инструментов, позволяющий захватывать снепшоты устройств, обрабатывать образы для восстановления данных, он предоставляет аналитические инструменты.

4. Для анализа и исследования сетевого трафика использовался инструмент Wireshark, а для исследования снепшотов памяти – LIME и Volatility.

На сегодняшний день доступны экспертные инструменты для анализа транзакций и кластеризации адресов, которые превращают криптотранзакции в простую визуализацию, подкрепленную точными данными об атрибуции адресов.

Заключение

По состоянию на 2022 г. в России запрещено использование криптовалют в качестве средства платежа, но при этом по-прежнему растут криптофинансовые потоки и незаконные финансовые сервисы на теневом рынке, в том числе и миксеры криптовалют. Между тем в Евросоюзе уже создан регулирующий орган AMLA, которому поручен прямой надзор за криптобизнесом.

При столкновении с биткойн-миксером, разработанным для сокрытия источника биткойнов и личности пользователей, правоохранительным органам требуется специфический набор навыков и инструментов для отслеживания средств, совершенно отличный от соответствующего комплекта для сбора криминалистических доказательств в случае более традиционных форм отмывания денежных средств. Кроме того, пока еще проведено мало исследований, направленных на рассмотрение и изучение криминалистического анализа сервисов смешивания биткойнов.

Аналитические платформы уже достаточно развиты для того, чтобы видеть все криптотранзакции. Примером является программное обеспечение Chainalysis для обеспечения соответствия требованиям в сфере оборота криптовалют. В России для этих целей работает платформа КОСАтка.

Не следует забывать, что использование Tor в Wasabi, как правило, помогает в решении проблем конфиденциальности и безопасности, но субъекты угроз, ищущие биткойн-трафик, могут и действительно нацеливаются на узлы Tor в попытках украсть средства или раскрыть пользователей.

В ближайшем будущем стоит ожидать появления криминалистических инструментов с применением поддельных нод Tor и дистанционным сбором свидетельств с хостов и облачных ресурсов для нужд криминалистической экспертизы. ●

Изъятие серверов злоумышленников и надлежащее восстановление информации помогают обеспечить значительную степень раскрытия анонимности этих транзакций.

В 2021 г. сотрудники Эдинбургского университета Нейпира опубликовали исследование, описывающее инструментарий и методологию для анализа сервисов смешивания биткойнов.

По состоянию на 2022 г. в России запрещено использование криптовалют в качестве средства платежа, но при этом по-прежнему растут криптофинансовые потоки и незаконные финансовые сервисы на теневом рынке.

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

[3] *https://www.napier.ac.uk/~/media/worktribe/output-2817546/a-blockchain-framework-in-post-quantum-decentralization-accepted-version.pdf*