Соколов Д.А., DOI 10.51980/2021_4_51

УНК ГУ МВД России по Челябинской области

Средства анонимизации, цифровые следы. Программный комплекс «Иолай»

В настоящее время при совершении преступлений, связанных с незаконным оборотом наркотических средств, причастные лица активно используют современные технологии, предназначенные как для дистанционной коммуникации, так и для анонимизации. Использование современных технологий позволяет участникам преступных групп сохранять анонимность и исключать личные встречи. Такой способ используется для непосредственной связи продавца и покупателя (передача адреса, фото, ссылки и др. с местом закладки), а также взаимодействия участников преступных групп, координации их действий. Таким образом, сотрудники полиции для эффективного решения оперативных задач должны постоянно следить за развитием современных технологий, своевременно их изучать и вырабатывать методы деанонимизации лиц, причастных к противоправной деятельности, как на этапе проверки информации о преступлениях, так и на этапе сопровождения уголовных дел.

К современным средствам анонимизации можно отнести следующие.

1. «Приватные» интернет-браузеры (например, TOR, Epic).

«Приватные» браузеры получили свое название благодаря тому, что они настроены таким образом, чтобы оставлять как можно меньше цифровых следов, при помощи которых может быть идентифицирован пользователь.

Часть из них могут иметь встроенные модули средств маршрутизации, о которых мы поговорим дальше. Одним из самых популярных браузеров, который в настоящее время имеет широкое распространение среди преступной среды, является TOR Browser.

2. Сервисы маршрутизации трафика (VPN, Proxy).

Оба варианта, как VPN, так и Proxy, позволяют осуществить маршрутизацию трафика, что в конечном итоге позволяет на «выходе» заменить реальный IP-адрес на IP-адрес сервера, который зачастую находится за пределами РФ.

Основным отличием при этом выступает то, что в случае с VPN трафик идет через специально создаваемый шифрованный тоннель, который является более защищенным от третьих лиц.

3. Удаленные серверы и иные виртуальные инфраструктуры (VPS/VDS). Использование данного спектра услуг позволяет злоумышленнику не хранить компрометирующие сведения на своем устройстве, но при этом иметь постоянный доступ к серверу при наличии под рукой любого устройства с доступом к сети Интернет.

4. Интернет-мессенджеры (Telegram, VIPole и др.). Миллионы людей ежедневно обмениваются сообщениями по всему миру. Но не многие задумываются о том, что происходит с сообщением, когда его отправляют, в отличие от правонарушителей, которые при выборе средств общения всегда ориентируются на следующие критерии:

– End-to-end шифрование (E2EE) – тип шифрования «сквозное»;

– степень централизации;

– возможность анонимного использования и регистрации (для регистрации аккаунта не требуются установочные данные, такие как абонентский номер телефона или адрес электронной почты клиента) – например, у мессенджера Pidgin.

5. Интернет-сервисы шифрованной передачи данных (Temp.pm, protonmail.com и др.). К данной категории сервисов относятся вспомогательные (дополнительные) средства, при помощи которых достигается повышенный уровень конфиденциальности. Как пример использования сервисов одноразовых самоуничтожающихся шифрованных сообщений – «Temp.pm», где пользователи имеют возможность создавать самоуничтожающиеся сообщения, которые будут ликвидированы после прочтения или после истечения таймера. Также в качестве примера можно привести почтовый сервис «protonmail.com», предлагающий безопасную переписку, защищенную сквозным шифрованием содержимого всех писем.

6. Сервисы обмена фотографиями. Существует множество сервисов для обмена файлами, но среди общей массы файловых обменников можно выделить фотохостинги. Так, на некоторых ресурсах не происходит переименование оригинальной фотографии, а другие и вовсе сохраняют имеющиеся у фотографий метаданные.

7. Различные финансовые инструменты (электронные платежные системы, криптовалюта). Финансовые инструменты условно можно поделить на такие категории, как цифровые валюты (далее по тексту – криптовалюты), электронные платежные средства и фиат.

Зачастую рассмотренные инструменты анонимизации комбинируются для достижения большей конспирации, но само по себе их

использование приводит к образованию различных цифровых следов.

Одними из ключевых способов деанонимизации являются сбор и анализ оставленных злоумышленником цифровых следов (пассивных и активных) при использовании различных интернет-ресурсов.

К пассивным следам можно отнести информацию об IP-адресе лица, которое осуществляло доступ к какому-либо из интернет-ресурсов, например загружало или просматривало фотографии на фотохостинге.

К активным следам можно отнести номер телефона или адрес электронной почты, оставленные лицом для получения доступа к какому-либо ресурсу, например при совершении обменных операций с криптовалютой.

Таким образом, можно говорить о том, что для эффективного установления лиц, причастных к противоправной деятельности, осуществляемой в информационно-телекоммуникационных сетях, их деанонимизации необходимо полное поэтапное фиксирование всех цифровых следов, имеющихся как на изъятых устройствах, так и на облачных хранилищах.

При работе по определенному интернет-магазину необходимо организовать постоянный мониторинг интернет-ресурсов, которые используются в его работе, начиная со способов оплаты за наркотические средства и получения потребителями адресов и заканчивая способами общения и обмена информацией.

Особое внимание стоит уделять фотографиям, размещаемым на фотохостингах и файловых обменных сервисах, которые помимо внешних признаков и цифровых следов в исходном виде могут содержать метаданные об устройстве, месте и дате съемки. Для сбора цифровых следов данной категории сложилась практика направления запросов об их предоставлении напрямую руководству сервисов. При получении ответов с конкретными IP-адресами целесообразно дальнейшее обращение к провайдеру для установления лица, его использовавшего. В таких запросах необходимо указывать диапазон IP-адресов, которому принадлежит интернет-ресурс.

Совокупность средств и способов получения данных на основе активных цифровых следов объединена в дисциплину, именуемую OSINT (Open source intelligence, в переводе с английского «разведка из открытых источников»).

При проведении OSINT используются следующие инструменты.

1. Поисковые сервисы.

У Google и Yandex есть несколько десятков команд для контекстного поиска, которые могут его облегчить, если знать, как ими пользоваться.

2. Приложения для определения принадлежности номера телефона.

Данные сервисы существуют за счет слитых баз данных о пользователях абонентских номеров либо другими пользователями, которые предоставляют приложению доступ к своим контактам. За счет этого база увеличивается в режиме реального времени. Не рекомендуется устанавливать подобного рода приложения на устройства, где имеются личные или служебные контакты. К наиболее популярным из таких сервисов относятся NumBuster, GetContact, Emobiletracker.

3. Проверка активности номеров.

Например, Smsc.ru. Это не единственный подобный сервис, но у него один из самых точных вариантов отправки как HLR-запросов, так и Ping-sms. Помимо активности показывает и принадлежность к региону и оператору (в том числе в случае перехода на другого оператора). При отправке Ping-sms на старые устройства может прийти сообщение, а при HLR-запросе такого не происходит.

4. Логирование ссылок, изображений – сервис IPlogger.ru. Иногда возникает ситуация, в рамках которой возможно поделиться с лицом, пытающимся скрыть личность в сети Интернет, файлом или ссылкой на какой-либо ресурс. В данной ситуации на помощь в деанонимизации могут прийти различные сервисы логирования. Одним из простейших является IPlogger.ru.

Принцип действия заключается в следующем: ресурс создает промежуточную ссылку между основным ресурсом и пользователем, при переходе по которой (или при открытии файла, в который она была помещена) происходит фиксация информации на серверах IPLogger, а именно IP-адрес, дата и время, версия браузера.

5. Многозадачные сервисы:

– Xinit.ru. Одним из наиболее функциональных бесплатных сервисов является ресурс Xinit. При помощи ресурса можно направлять массовые запросы на принадлежность номера телефона к номерной емкости, массовые запросы по IP-адресам на принадлежность провайдеру, запросы по доменным именам, банковским картам, координатам базовых станций и даже Wi-Fi точек доступа;

– инфосфера. Сервис осуществляет проверку физических лиц, номеров телефонов, e-mail и организаций. Поиск осуществляется по данным из 70 источников;

– интернет-розыск. Многозадачный сервис, включающий в себя проверку по IP-адресам, по номерам телефонов, адресам электронной почты, аккаунтам мессенджера Telegram.

6. Telegram-боты для проведения OSINT.

Ввиду того, что многие из OSINT-сервисов работают по API, многие из них подключены к различным Telegram-ботам, которые

значительно экономят время на проверку. Telegram-боты функционируют также и с другими базами, которые не всегда имеются в свободном доступе или же довольно объемны для работы на персональном компьютере или телефоне. К таким Telegram-ботам относятся: @buzzim_alerts_bot (осуществляет поиск сообщений по каналам); @HowToFind_RU_bot (разноплановый инструмент многоцелевого поиска); @egrul_bot (по пользовательским запросам выдает информацию о юридических лицах, ИП); @EyeGodsBot (поиск по фото, по номеру телефона, по номеру автомобиля, по профилю в социальных сетях и иным источникам).

7. Сервисы, осуществляющие анализ профилей пользователей социальных сетей. Это автоматизированные системы круглосуточного мониторинга и сбора данных из сети Интернет, позволяющие получать и анализировать широкий спектр информации из социальных сетей (например, Facebook, «ВКонтакте», «Одноклассники», Instagram), микроблогов Twitter, онлайн-СМИ, а также из персональных блогов «Живого журнала» и мессенджера Telegram. К таким сервисам относятся «Крибрум», «Демон Лапласа», «Сеус Лаб».

В качестве заключительного примера необходимо рассмотреть программный комплекс «Иолай».

Говоря о том, что в настоящее время большая часть сбыта наркотических средств перешла в теневой Интернет, отдельно следует упомянуть ресурс Hydra, являющийся крупнейшей интернет-площадкой по продаже наркотических средств на территории Российской Федерации и стран СНГ. Данный интернет-ресурс расположен в домене onion, доступен только из браузера TOR. Доля продаж наркотических средств через Hydra, что касается интернет-пространства, составляет порядка 70-80%. Магазины, осуществляющие деятельность по продаже наркотиков, размещенные на ресурсе Hydra, принимают к оплате только криптовалюту биткойн.

Для помощи сотрудникам полиции в борьбе с преступлениями в сфере незаконного оборота наркотиков был создан программный комплекс «Иолай», предназначенный для анализа складывающейся оперативной обстановки на территории обслуживания. Программный комплекс позволяет в режиме реального времени осуществлять мониторинг интернет-площадки Hydra, загружать информацию о количестве интернет-магазинов, представленных данным ресурсом на территории Российской Федерации, ассортименте предлагаемых ими наркотических средств, ценах, городах в которых представлены интернет-магазины, с возможностью просмотра указанной информации в интересующий промежуток времени с момента начала работы программного комплекса.