Ненашев Е.В.

Дальневосточный юридический институт МВД России (г. Хабаровск)
Научный руководитель А.С. Пудовиков, кандидат юридических наук, доцент

Технические данные об устройствах-инициаторах, сохраняемые в базах данных кредитных организаций, как важнейший источник криминалистически значимой информации, получаемой в ходе расследования краж, совершенных с банковских счетов

Одной из ключевых задач при расследовании преступлений является установление местонахождения и личности подозреваемого лица. В случаях расследования краж, совершенных с банковских счетов, а равно в отношении электронных денежных средств, особенно когда они были совершены дистанционно, то есть без непосредственного контакта с потерпевшим или его банковской картой, установить местонахождение и личность подозреваемого практически невозможно из-за использования последним современных средств как анонимизации своей персоны, так и маскировки похищенных денежных средств.

С целью выяснения наиболее проблемных для расследования способов сокрытия преступных следов нами было проведено анкетирование сотрудников из различных регионов ДФО (Хабаровский край, Камчатский край, Республика Саха (Якутия), Приморский край и др.), осуществляющих расследование и раскрытие преступлений в сфере информационно-телекоммуникационных технологий. Одним из вопросов, представленных 51 сотруднику, был следующий: какой из представленных способов сокрытия следов со стороны преступника, по вашему мнению, требует наибольшей активизации? Возможно было выбрать несколько вариантов, которые, по мнению анкетируемого сотрудника, являются требующими наибольшего внимания, по итогу опроса были достигнуты следующие результаты:

– использование банковских карт, оформленных на других лиц: указали 4 респондента;

– использование средств IP-телефонии: указали 35 респондентов;

– использование оформленных на других лиц сим-карт: указали 7 респондентов;

– использование преступниками прокси-серверов: указали 16 респондентов;

– размер цепочки банковских счетов, ведущих к основному мастер-счету: указали 8 респондентов;

– использование мобильных и компьютерных устройств со специальной аппаратной прошивкой, блокирующих возможность определения местоположения: указали 17 респондентов;

– использование поддельных страниц в социальных сетях и онлайн-сервисах: указали 4 респондента.

Согласно опросу наиболее «острыми» способами сокрытия следов являются использование преступниками средств IP-телефонии (68%), мобильных и компьютерных устройств со специальной аппаратной прошивкой, блокирующих возможность определения местоположения (33%), прокси-серверов (31%), цепочки банковских счетов, ведущих к основному мастер-счету (15%), оформленных на других лиц сим-карт (14%), подложных банковских карт и поддельных страниц в социальных сетях и онлайн-сервисах (8%).

Согласно представленному опросу наиболее проблемными для опрошенных сотрудников оказались сетевые и коммуникативные средства обеспечения анонимизации. И все же в рамках данного исследования, мы хотели бы частично абстрагироваться от указанных способов анонимизации и сделать больший акцент на банковских средствах. Исследуя работы ученых-криминалистов в области развития методики расследования хищений с банковских счетов, можно столкнуться с некоторой недооценкой возможностей запросов, направляемых в кредитные организации. Так, зачастую перечень вопросов ограничен необходимостью предоставить только выписки о движении денежных средств с указанием времени и даты трансакций, анкетных данных держателей счетов, а также о наличии иных счетов и банковских карт, открытых на установочное лицо. Однако существует еще один важный аспект, который также необходимо выяснять в рамках тех же запросов в кредитные организации.

В данном случае мы хотели бы акцентировать внимание на дополнительной возможности в идентификации подозреваемого лица, заключенной также в информационных сетях банков. Согласно п. 7.17 Стандарта Банка России СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств»[1] для событий информационной безопасности банки сохраняют различную сетевую информацию. Применительно к указанному исследованию нас интересуют следующие пункты сохраняемой информации:

– информация о результатах установления и отклонения прокси-соединений;

[1] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств : Стандарт Банка России СТО БР ИББС-1.3-2016 : принят и введен в действие приказом Банка России от 30.11.2016 № ОД-4234 // СПС Гарант.

– информация VPN-шлюзов об установлении взаимодействия на сетевом уровне, в том числе IP-адреса источника и получателя данных, дата и время обработки сетевых пакетов;

– информация об IP-адресе инициатора запроса;

– информация о веб-браузере, сформировавшем запрос;

– информация об операционной системе средства вычислительной техники, использованного для формирования запроса.

Перечисленные выше сведения могут быть использованы для дополнительной идентификации подозреваемого лица, особенно в тех случаях, когда преступник восстановил доступ к банковскому приложению, использовав полученные от потерпевшего конфиденциальные сведения о его банковской карте с кодом из PUSH-уведомления. Восстановив таким образом доступ к личному кабинету потерпевшего, преступник может самостоятельно осуществить все необходимые ему трансакции.

Важной уязвимостью такого способа совершения хищения является необходимость использования какого-либо устройства (смартфона, персонального компьютера, планшета и т.д.) с предустановленным банковским приложением. Поскольку такие приложения осуществляют работу только при подключенном интернет-соединении, следовательно, сами устройства оборудованы сетевой картой или чипом, обладающими своим уникальным MAC-адресом. Кроме того, для подключения интернета преступнику необходимо приобретать услуги провайдера, который определяет IP-адрес клиента (даже в случае динамического IP-адреса возможна аналогичная идентификация). В итоге, восстановив доступ в личный кабинет потерпевшего через банковское приложение согласно представленному Стандарту Банка России, банковские системы безопасности фиксируют сведения об устройстве, с которого был осуществлен вход в приложение, ввиду чего мы можем узнать дополнительные сведения о самом преступнике. Фиксируются также сведения о том, использует ли преступник VPN или прокси-сервер. Сведения же об IP-адресе и MAC-адресе могут позволить идентифицировать местоположение преступника, нивелируя другие способы маскировки своей личности и местоположения. Кроме того, получив таким образом сведения о местоположении и личности преступника, возможно сравнивать их с другими сведениями, полученными из других ответов на запросы или результаты оперативно-розыскной деятельности, с целью выявления более глубоких информационных пробелов в системе безопасности преступников.