со сторонней системы не получится войти в аккаунты подозреваемого даже имея логины и пароли.

Таким образом, проведение обыска по делам, связанным с криптовалютами, имеет свои особенности. Указанные выше действия, способствуют сохранению электронно-цифровых следов и доказательств, которые могут быть уничтожены, способствуют выявлению преступлений и привлечению виновных к уголовной ответственности.

Шнейдерова Д. И.

СЕРВИСЫ-АНОНИМАЙЗЕРЫ КАК СРЕДСТВА СОКРЫТИЯ ЛИЧНОСТИ ПРЕСТУПНИКА ПО ДЕЛАМ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

Шнейдерова Дарья Игоревна, аспирант Белорусского государственного университета, г. Минск, Беларусь, galuzodi@mail.ru

Научный руководитель: канд. юрид. наук, доцент Асаёнок Б. В.

Практическая невозможность установления личности преступника по уголовным делам о хищениях в сфере оборота криптовалют – ключевая проблема, образующая низкий процент раскрываемости указанной категории преступлений, которая вызвана использованием киберпреступниками специализированных сервисов, позволяющих осуществлять противоправную деятельность через сеть Интернет анонимно для сторонних пользователей и правоохранительных органов, т. е. с сокрытием реального IP-адреса используемого в этих целях устройства. Среди таких сервисов можно выделить механизмы маршрутизации NAT и DHCP, VPN-сервер, прокси-сервер SOCKS и TOR-маршрутизатор.

Технологии NAT и DHCP, применяемые крупными интернет-провайдерами, позволяют скрывать фактическое количество IP-адресов устройств, выходящих в сеть, тем самым образуя диссонанс между реальным количеством пользователей и адресами тех устройств, которые доступны для анализа трафика сети. Так, технология NAT присваивает один и тот же внешний IP-адрес нескольким устройствам, выходящим в интернет, при этом сохраняя внутренние IP-адреса в специальной переводной таблице с целью последующего обеспечения правильной маршрутизации ответного входящего пакета данных. Технология DHCP действует в противоположном порядке – присваивает одному внутреннему IP-адресу несколько краткосрочных внешних адресов, что позволяет считать активность одного лица в сети как деятельность разных пользователей.

VPN выступает разновидностью частной виртуальной сети, позволяющей своим клиентам выходить в интернет не под адресом своего устройства, а под IP сервера VPN, шифруя при этом трафик подключения пользователя к VPN-сервису и лишая провайдера возможности анализа активности пользователя в

сети. Для киберпреступников, осуществляющих хищения криптовалют, характерно использование усовершенствованной двухсерверной технологии – Double VPN, которая обеспечивает двойную степень анонимности пользовательского устройства. Так, преступник первоначально подключается к «публичному» серверу VPN (данное подключение доступно для видимости и анализа провайдером), а затем перенаправляется ко второму «приватному», под IP-адресом которого и действует в сети Интернет анонимно. Однако если провайдер отследить активность конкретного пользователя, использующего VPN, не может, то данная функция доступна владельцам сервера VPN, что при определенных обстоятельствах не совпадает с желаниями пользователей в области обеспечения абсолютной анонимности. В связи с этим в качестве третьего уровня защиты преступниками используется SSH-тоннель, который принимает пакеты данных от Double VPN и через тоннель перенаправляет их конечному адресату. При таких обстоятельствах, если VPN обеспечивает шифрование трафика от провайдера, то SSH – от сервера VPN. Упрощенной технологией, по сравнению с VPN, выступает прокси-сервер SOCKS, который обеспечивает передачу данных от одного пользователя другому под своим IP (т. е. выступает посредником), но при этом не шифрует трафик передачи данных, что может отслеживаться провайдером сети.

Маршрутизатор TOR, используемый в одноименной виртуальной сети, открывающей доступ к «теневому» сегменту сети Интернет – DarkNet, имеет свой домен верхнего (.onion) и базируется на механизме передачи данных через цепочку случайных узлов, подключенных к сети («луковая» маршрутизация). Принцип работы TOR-маршрутизации можно представить следующим образом: первый исходный узел (отправитель) формирует пакет данных, шифруя его тремя публичными ключами доступа (т. е. накладывая «луковые» слои защиты). Готовый пакет перенаправляется второму случайному узлу сети (входной), который своим ключом снимает первый слой шифрования и передает данные третьему транзитному узлу, выполняющему ту же операцию и пересылающему пакет к четвертому узлу – выходной ноде. На выходной ноде данные окончательно расшифровывают и отправляются конечному получателю – пятому узлу. Такая система шифрования и вовлечения случайных узлов в процесс передачи трафика позволяет обеспечивать анонимность пользователей внутри сети TOR.

Таким образом, IP-адрес устройства выступает ключевым элементом при анализе активности пользователя в сети Интернет и сборе образуемых от нее «цифровых» следов, анонимизирование которого путем использования рассмотренных сервисов и механизмов не позволяет правоохранительным органам получить криминалистически значимую информацию, ведущую к установлению личности лиц, совершивших хищения в сфере оборота криптовалют, что связано с регистрацией таких сервисов на территории иностранных государств и их отказом в связи этим от предоставления информации о своих клиентах.