Секция «Информационное общество, цифровая экономика и информационная безопасность»

Значение использования специальных знаний в доказывании хищения персональных данных клиентов в банковской сфере

Научный руководитель – Макаренко Мадина Муссаевна

Пронин Даниил Николаевич
Студент (специалист)
Московский университет Министерства внутренних дел Российской Федерации,
Факультет подготовки следователей, Москва, Россия
E-mail: sergeantmoroz@gmail.com

Первое с чем следует разобраться при начале предварительного следствия, так это с предметом преступления. Для обозначенной темы предметом являются персональные данные клиентов платежных систем, в том числе и банковских. Итак, персональные данные - это любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту персональных данных, в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, данные паспорта (серия, номер, когда и кем выдан документ); номер мобильного телефона; другие данные [Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных"//Собрание законодательства РФ. 31.06.2006. № 31. ст. 3451].Информация, а именно персональные данные клиентов, хранится на отдельных защищенных серверах, отличающимся по алгоритмам от той защиты, что стоит на остальных банковских хранилищах электронной информации.

Для предметного рассмотрения вопроса выделить ряд непосредственных угроз безопасности:

1)Несанкционированный доступ представляет собой получение доступа к ресурсу, на который у злоумышленника нет разрешения.

2)Атака «Салями». Принцип работы этого метода состоит в постепенном сборе дробных чисел. При обработке счетов используются целые единицы, а те самые дроби образуются при начислении процентов. И схема работает на округлении дробных процентных сумм в пользу злоумышленника. Таким образом, чем больше оборотные средства, тем больше прибыль хакера.

Успех таких атак зависит не от количества денег, украденных со счета потерпевшего, так как для любого счета погрешность обнуления одинакова, а от количества обработанных операций. Атаки «салями» довольно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете крупные суммы.

3) Сборка мусора т.е. восстановление данных не подвергнутых физическому уничтожению или подготовленных к стиранию. Данная процедура проводится как на дисках компьютера, так и в оперативной памяти. Для осуществления данной операции, программа маскирует свои действия под нейтральный процесс, тем самым выделяя под свои нужды необходимую часть оперативной памяти.

Далее злоумышленник с помощью заранее загруженного кода просматривает сектора памяти компьютера на предмет подготовленных к удалению или уже удалённых, но всё ещё пригодных для восстановления данных, содержащих нужные взломщику ключевые слова. Так восстанавливая удаленные данные, злоумышленник получает доступ к информации о соединениях, а в случае использования незащищенных или слабо защищенных платежных систем к данным о платежах, в том числе и платежные реквизиты, а так же логин и пароль платежного сервиса, которым пользовался потерпевший.

К данным такого рода относятся и личные идентификаторы. В системах онлайн-банкинга проводится аутентификация по комбинации логина, пароля и одноразового кода подтверждения перехват которой позволяет выполнять действия от имени пользователя. Также в веб-приложениях существует возможность кражи cookie-файлов (идентификаторов сессий), подобное действие позволяет воспользоваться данными реального пользователя, который авторизировался в системе ранее легальный способом. И хотя банки используют достаточно надёжные системы защиты, данные всё ещё можно украсть. Обычно для этого используются вредоносные программы, которые несанкционированно внедрены на устройство пользователя.

Главным доказательством незаконной деятельности взломщика являются результаты компьютерно-технической экспертизы. Следователь в рамках своей деятельности должен грамотно Сформулировать вопросы, которые подлежат разрешению в рамках данной экспертизы и не выходят за пределы компетенции эксперта. Кроме того, эксперту необходимо представить пригодные для исследования материалы. Так, например, для доказательства факта установки на устройство вредоносного программного обеспечения, требуется изъять дисковый носитель, в памяти которого непосредственно установлено нелегальное программное обеспечение. Одновременно с изъятием носителя у потерпевшего следует направить оперативным сотрудникам поручение на проведение ОРМ «Получение компьютерной информации» в отношении владельца IP-адреса, обнаруженного в ходе осмотра электронного почтового ящика потерпевшего, а именно находящегося в нём электронного письма, содержащего фишинговую ссылку [Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 02.08.2019) "Об оперативно-розыскной деятельности"// Собрание законодательства РФ №33 от 14.08.1995, ст. 3349].

Далее после получения результатов ОРМ в виде дискового носителя, принадлежащего злоумышленнику, на котором записан оригинал вредоносной программы, представить его для экспертного исследования.

Особенности механизма совершения кражи персональных данных таковы, что охарактеризовать их может только эксперт в своем заключении. Учитывая это обстоятельство, следователь должен грамотно изъять вещественные доказательства, а именно с привлечением эксперта. Так как злоумышленник может оставить в компьютерной системе или на самом изымаемом носителе информации «ловушку», которая при несанкционированной попытке доступа уничтожит хранящиеся на носителе данные.

При назначении различных видов экспертиз, в зависимости от цели их проведения, перед специалистом целесообразно поставить следующие вопросы:

1) аппаратно-техническая экспертиза-

- пригодны ли предоставленные на экспертизу носители информации для исследования;

- каким способом было осуществлено внедрение вредоносного ПО в систему потерпевшего;

2) компьютерно- техническая экспертиза,-

- имеются ли в представленном на экспертизу дисковом носителе отклонения от типовых (нормальных) параметров, в т.ч. физические дефекты;

- имеются ли на компьютере, представленном на экспертизу, программные средства для реализации внедрения вредоносного ПО;

- каков состав файлов дискового носителя представленного на экспертизу, каковы их параметры (объемы, даты создания, атрибуты);

3) программно-компьютерная экспертиза,-

- можно ли определить реквизиты разработчика и владельца представленного программного средства, если да то каковы они;

- какое общее функциональное предназначение имеет программное средство;

- используется ли данное программное средство для кражи персональных данных;

- имеются ли в программном средстве компьютера какие-либо враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютерной системы;

- какого вида (явный, скрытый, удалённый, архив) имеется информация на носителе;

-каким образом организован доступ (свободный, ограниченный и пр.) к данным на носителе информации и каковы его характеристики;

- какие признаки преодоления защиты (либо попыток несанкционированного доступа) имеются на носителе информации;

- какие данные о пользователе компьютерной системы (в т.ч. имена, пароли, права доступа) имеются на представленном носителе;

- каким способом и при каких обстоятельствах произведены действия (операции) (блокирование, модификация, копирование, удаление) определённых данных на носителе информации (компьютере);

- какая хронологическая последовательность действий с внедренных программным обеспечением имела место при краже персональных данных;

- какая имеется причинная связь между действиями, а именно вводом вредоносного ПО на носитель и имевшим место похищение персональных данных потерпевшего.

Изложенные аспекты актуализируют значение использования специальных знаний и в обязательном порядке должны учитываться следователем в ходе расследования уголовных дел, возбужденных по фактам совершения хищений персональных данных клиентов банковской сферы.

Источники и литература

1) Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных"//Собрание законодательства РФ. 31.06.2006. № 31. ст. 3451.

2) Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 02.08.2019) "Об оперативно-розыскной деятельности"// Собрание законодательства РФ №33 от 14.08.1995, ст. 3349