И на десерт, ко всем этим неожиданным списания, выяснилось, что никакой брони в авиакомпании нет и не было. Т.е. авиабилеты не были забронированы. Все было обманом и деньги ушли в неизвестном направлении.

В результате с карты украли (потери за оплаченные билеты и последующие списания) в общей сумме составили 47 377рублей. А могло бы быть гораздо больше.

Теперь попробуем разобраться, что же на самом деле произошло и где можно было обнаружить подвох.

1. Домен в зоне EU должен был по крайней мере насторожить.

2. Кроме поиска авиабилетов на сайте было всего несколько страниц, цель которых пустить пыль в глаза.

3. Если копнуть глубже, то указанный на странице ОГРН компании принадлежал компании, которая была закрыта в 2011 году. А само название компании в выписке ЕГРЮЛ и на сайте не совпадает, на сайте частично изменено. Проверить данные по ОГРН, ИНН и названию юридических лиц можно в базе налоговой инспекции egrul.nalog.ru.

4. Рейтинги сайта ТиЦ и PR нулевые (это видно в тех редких случаев, когда в браузере установлена панель вебмастера или что-то похожее).

5. Основное, что должно было насторожить. Должна была быть оплата без комиссии, как указано на сайте, 5900 за каждый авиабилет, а в смс от банка пришло назначение «Списание 5900.00 P2P PSBANK», а после оплаты этих 5900, приходила смс о том, что списано 5988,50р. Что такое «P2P» конечно знают не все. Можно было бы поискать. «P2P» — это сервис перевода с карты на карту. А сумма списания больше, чем сумма платежа, потому что банк, через который производился платеж, берет за это комиссию. Т.е. реально деньги, которые якобы оплачивались за авиабилеты, переводились на чью-то банковскую карту через сервис PSBANKa (Промсвязьбанк). При этом покупателю банк присылал проверочный код 3D Secure, который покупатель, ничего не подозревая, вводил в браузере.

6. Если с переводом на карту для меня понятно, что владельца карты ввели в заблуждение, чтобы он сам ввел код 3D Secure, то с последующими списаниями без проверки 3D Secure, для меня ситуация не совсем понятна. Я ни разу не сталкивался с ситуацией, чтобы Сбербанк в интернете позволял что-то оплатить без проверки 3D Secure (без подтверждения через SMS). Единственный исключение, когда смс не запрашивается, — это когда операции производятся через мобильное приложение СбербанкОнлайн на телефоне. Но телефон похищен не был и данные от личного кабинета похищены не были. Очевидно, что были получены только данные банковской карты моего знакомого. И, имея только данные карты, деньги списывались при использовании сервиса YM (Yandex.Money) в пользу Yandex.Direct (рекламная сеть Яндекса). Здесь есть явно какая-то недоработка в системе безопасности и возникает вопрос либо к Сбербанку, либо к Яндексу, как они такое позволяют делать.

В результате складывается примерно такая картина работы мошеннического сайта:

Сайт через рекламу в Яндекс.Директ привлекает посетителей. Без рекламы таким сайтам выбраться в топ выдачи практически нереально. Выглядит сайт в чем-то похожим на нормальные сайты. Поиск рейсов и свободных мест работает отлично. Для этого сайт принимает запрос посетителя, просит его подождать, сам отправляет запрос на какой-то другой сайт, на котором есть реальные данные по авиабилетам, из полученного ответа вырезается лишнее и подготовленная информация выдается на своей странице. Вполне возможно, что и цены немного корректируются (цены я не проверял). Дальше посетитель оформляет заказ, вводя свои данные. Ввод данных выглядит также, как и на многих других сайтах по продаже билетов. После ввода данных и подтверждения заказа, покупателю сообщают код заказа и дают 24 часа на оплату. При оплате оригинальная страница одного из банков с сервисом перевода P2P переделывается определенным образом (об этом ниже) и встраивается на мошеннический сайт. «Покупатель» авиабилетов, если не заметит подвох, переводит деньги на какую-то чужую банковскую карту. При этом данные банковской карты «покупателя» перехватываются и в дальнейшем используются для списаний — при этом пополняется счет какого-то аккаунта в Яндекс.Директ для последующей рекламы и поиска новых жертв. Дальше все тоже самое по кругу.

После всей этой истории было написано заявление в полицию (на рассмотрении), в сбербанк (на рассмотрении), в Яндекс, хостинг-провайдеру и др.

Мошеннический сайт размещался на хостинге FirstVDS. По моему заявлению с подробным описанием аккаунт мошеннического сайта заблокировали. Правда, через

полдня опять разблокировали. Но по повторному заявлению опять заблокировали (надеюсь, уже навсегда), сославшись на то, что разные отделы провайдера не разобрались. Конечно, это не полная блокировка — мошенники могут поменять хостинг.

Одержав хоть маленькую и временную, но победу с закрытием сайта, нужно было решать вопрос с авиабилетами. И какого же было удивление, когда по аналогичному поисковому запросу Яндекс на первой строчке рекламного блока выдал другой сайт, который имел слегка измененный дизайн, но имел практически тот же функционал и похожий движок. Его цель — обман посетителей, кража денег и данных кредитных карт. Т.е. задушив один сайт, тут же появляется новый сайт (точнее он и раньше работал, просто в рекламе поднимаются не все сразу). Адрес другого сайта, по «якобы продаже авиабилетов» — _avia-scanners.ru_. Если представители Яндекса захотят проверить, то вот полная ссылка из Яндекс.Директа (в которой есть идентификатор рекламодателя.

Read Full Article