История успеха

Защита от интернет-мошенничества на всех ключевых ресурсах. Опыт работы с Туту.ру

tutu.ru

Туту.ру — онлайн-сервис путешествий, работающий с 2003 года. На Туту.ру можно купить билеты на поезд, электричку, самолет и автобус, забронировать гостиницу и приобрести тур. Ежедневно Туту.ру посещают 1 миллион человек.

Обнаружившаяся проблема

Сотрудники компании Туту.ру начали получать жалобы от клиентов, которые встречали в Интернете фишинговые сайты, паразитирующие на бренде Туту.ру. В частности, подобные сайты мимикрировали под один из продуктов или название онлайн-сервиса, предлагали купить билеты с 70% скидкой. Естественно, никаких реальных билетов эти лжесайты не имели и не продавали. Они пытались таким образом лишь похищать данные клиентов.

Оборона своими силами

Ситуация осложнялась тем, что ежедневно сайт Туту.ру посещает 1 миллион человек, и каждый из них потенциально мог пострадать.

Туту.ру предпринимали попытки защитить репутацию своего бренда самостоятельно: выявляли, откуда идет парсинг данных - злоумышленники должны были что-то показывать клиентам - и блокировали эти адреса. Но это имело временный эффект, и сайты оживали с завидным постоянством. Специалисты внутренних департаментов взаимодействовали, в том числе с регистраторами, хостинг-провайдерами и рекламными сетями, но, по словам Вадима Мельникова, технического директора Туту.ру, это оказалось «долго, мучительно и малоэффективно».

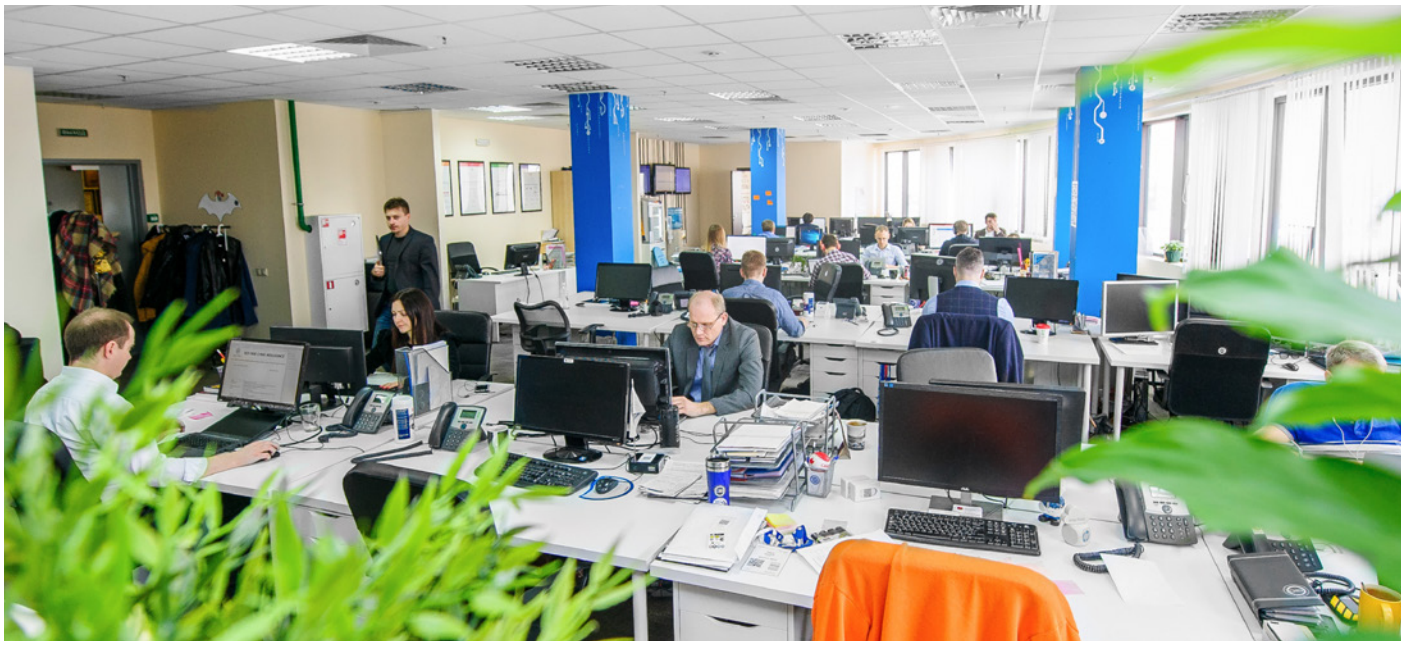
В итоге стало ясно, что решать обнаружившуюся проблему силами сотрудников компании нецелесообразно: отдельного департамента, занимающегося подобными вопросами в организационной структуре компании нет, а время сотрудников, которые в силу прямых своих обязанностей сталкиваются со злоупотреблениями, эффективнее тратить на более важные для бизнеса задачи.

Суть мошенничества:

Злоумышленники копировали внешний вид сайта (либо разовачивали его внутри фрейма) и размещали по схожему URL-адресу. Затем, создавали рекламные объявления в поисковых системах Google и Яндекс. В тексте объявления указывали настоящий домен, который после модерации объявления незаметно подменялся на фишинговый.

Схожим образом действовали и с мобильными приложениями, копируя оригинальный дизайн и размещая ссылки на скачивание клонов как с официальных, так и с неофициальных площадок в группах соц. сетей и контекстной рекламе. После устновки приложений пользователи теряли персональные данные, а в некоторых случаях и деньги.

> **Проблема возникла ещё в 2015 году. Прислушавшись к рекомендациям коллег из индустрии мы решили обратиться в Group-IB Brand Protection. После проведения пилотного проекта остались довольны и начали сотрудничество, которое продолжаем до сих пор.**
>
> **Вадим Мельников,**
> Технический директор Туту.ру



Что сделали в Group-IB

Для защиты бренда Туту.ру от мошеннических действий злоумышленников мы предложили решение Brand Protection.

- **Выявили более 12 000 доменных имен, созвучных или схожих с Туту.ру.**

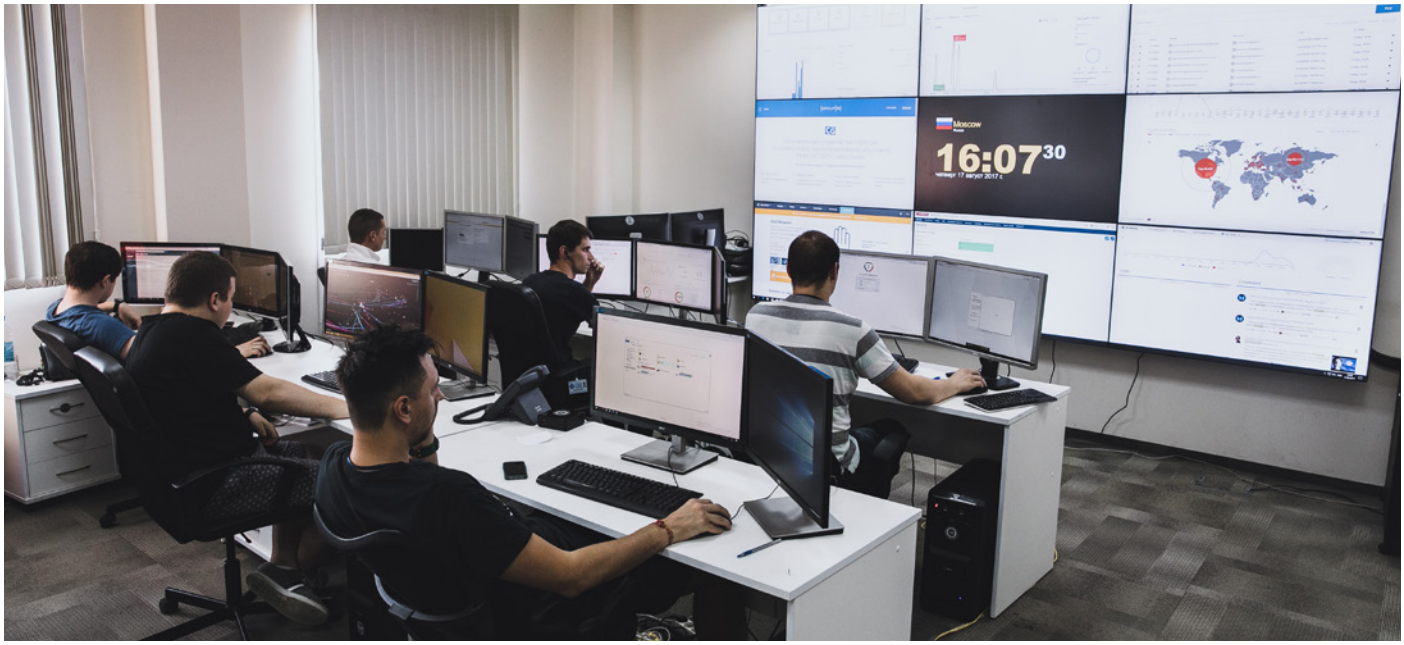
  Мы сотрудничаем с крупными регистраторами доменных имен, которые регулярно предоставляют информацию по новым сайтам в зоне .ru и .рф. Благодаря этому у нас всегда есть база функционирующих доменов. Чтобы находить домены третьего уровня или в определенной географической зоне, мы используем технологию пассивного DNS. Она представляет собой сбор данных о совершающихся DNS-запросах.

- **Проанализировали сопряжённые сайты по степени риска и составили очередность реагирования.**

  Если на каких-то ресурсах находили реальные угрозы, инициировали мероприятия по блокировке. Даже если в момент обнаружения сопряженных ресурсов признаки мошенничества отсутствовали, мы все равно оставляли их на автоматическом мониторинге. Поэтому, едва только злоумышленник решал воспользоваться доменом под именем Туту.ру, мы в ту же минуту об этом узнавали и принимали меры.

- **Выявили более 2 000 рекламных объявлений и мобильных приложений, направленных на сервис Туту.ру.**

  Несмотря на то, что не все они были мошенническими изначально, каждый ресурс оставался на регулярной автоматической проверке, поскольку любые подобные предложения представляют потенциальную угрозу бренду.



Результаты работы Group-IB Brand Protection

- **Заблокировали 100% ресурсов, которые могли нанести или наносили ущерб бренду и его клиентам:**
  - 150 сайтов и вредоносных мобильных приложений
  - противоправный контент на ресурсах, нарушающих права Туту.ру.
- **Вернули трафик на официальный сайт Туту.ру**

- **Заблокировали 150 сайтов**
- **Выявили 12 000 созвучних доменных имен**
- **Выявили и поставили на слежение 2 000 рекламных объявлений и мобильных приложений**

> **Компания Туту.ру заботится о своих клиентах и стремится оградить их от финансовых потерь. Лояльные клиенты онлайн-сервиса путешествий не будут введены в заблуждение мошенниками, использующими со злым умыслом имя Туту.ру.**

Вадим Мельников,

Технический директор Туту.ру

Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защиты интеллектуальной собственности в сети.

В основе решения Brand Protection — собственные разработки для борьбы с киберпреступлениями и уникальные данные киберразведки. Постоянное развитие механизмов обнаружения нарушений позволили защитить более 200 российских и зарубежных брендов

По версии **Gartner, IDC и Forrester,** Group-IB является одним из ключевых поставщиков Threat Intelligence в мире, в базе которой хранится 100 000+ профайлов киберпреступников.

55 000+

часов реагирования

1000+

расследований по всему миру

EUROPOL INTERPOL **Официальный партнер**

OSCE **Рекомендована Организацией по Безопасности и Сотрудничеству в Европе (ОБСЕ)**

Узнайте больше об услуге Brand Protection:

group-ib.ru/brandprotection

info@group-ib.com