OSHALiANG
Intellectual Property Law

Кибersквоттинг: опасен для любого бизнеса

Введение

Кибersквоттинг стал одной из самых серьезных проблем, с которой сталкиваются компании США, работающие с потребителями. Кибersквоттинг может принимать разные формы, но его цель всегда одна — кража денег или ценной личной информации у ничего не подозревающих пользователей. Мошенники часто используют распространенные ошибки в написании доменных имен, торговую марку и цветовую схему существующих компаний, чтобы ввести потребителей в заблуждение.

Кибersквоттинг может нанести огромный ущерб любой компании. Например, пользователи, ставшие жертвами кибersквоттинга, но не подозревающие об этом, могут негативно отзываться в социальных сетях, рассылках и печатных изданиях о законном бизнесе, название которого использовали преступники. Кроме того, жертвы кибersквоттинга не рискуют снова обращаться в компанию со схожим названием, поэтому легальный бизнес терпит убытки даже тогда, когда его репутация не страдает. Кибersквоттеры постоянно совершенствуют свои методы, и количество фальшивых сайтов неуклонно растет.

Проблему углубляет и то, что найти преступника может быть очень сложно. Кибersквоттеры умело скрывают свою личность, используя так называемые веб-прокси — сервисы, позволяющие скрыть домен. Несмотря на это, существуют несколько стратегий, позволяющих с помощью опытного юриста и авторских прав на интеллектуальную

собственность решить связанную с кибersквоттингом проблему. Эта статья посвящена наиболее распространенным методам кибersквоттинга[1].

1. Фишинг-мошенничество по электронной почте

Злоумышленники используют электронный адрес, чтобы выдать себя за представителей существующей компании. Кибersквоттер отправляет потенциальному клиенту такой компании электронное письмо с предложением о сотрудничестве и запросом финансовой информации. Представившись сотрудником определенной компании, мошенник может попросить у пользователя личную информацию под предлогом восстановления клиентского аккаунта или предоставления мини-кредита. С помощью украденной информации кибersквоттер получает доступ к финансовым счетам жертвы или открывает новые счета на ее имя.

2. Тайпсквоттинг

Кибersквоттеры регистрируют доменное имя, близкое по написанию к веб-адресу настоящей компании. Как правило, доменное имя мошенников — это неправильно написанное название существующей компании, содержащее распространенную опечатку. Сайт, который потребитель найдет по этому адресу, настолько похож на нужный интернет-ресурс, что заметить подделку очень сложно. Обычно сайт тайпсквоттера предлагает посетителю те же услуги, что и настоящая компания, используя ее торговую марку, фирменное оформление и даже тот же стиль общения с клиентами. Злоумышленник стремится получить личную информацию потребителя, например, чтобы открыть кредит на его имя или получить доступ к его финансовым счетам. Иногда

[1]Для краткости некоторые примеры в статье объединены и попадают под определение кибersквоттинга, хотя, строго говоря, им не являются.

тайпсквоттеры используют сайт с содержащим опечатку веб-адресом, чтобы с него перенаправить пользователя на другой принадлежащий кибersквоттеру сайт.

3. Мошеннические веб-страницы на доменах, не нарушающих авторские права

Кибersквоттеры могут использовать программное обеспечение, чтобы создать ссылки на веб-страницы, которые отображаются по-разному в зависимости от того, по какой ссылке перешел пользователь. Этот метод позволяет злоумышленнику зарегистрировать доменное имя, не нарушающее авторские права. На подстраницах такого сайта пользователю предложат услуги под торговой маркой и названием компании, за представителей которой выдают себя кибersквоттеры. Например, мошеннические ссылки могут вести на несколько страниц, каждая из которых содержит предложение о мини-займе от одного из трех крупнейших кредитных учреждений США. Однако корневой домен такого сайта не нарушает ничьи авторские права. Для обычных компаний такой случай кибersквоттинга особенно опасен, потому что мошенник является законным владельцем домена и не попадает под действие Единой политики разрешения доменных споров (UDRP). Чтобы подробнее узнать о процедурах UDRP, посетите веб-сайт Интернет-корпорации по присвоению имен и номеров: https://www.icann.org/resources/pages/policy-2012-02-25-en.

4. Доменные имена, предлагающие фальшивые услуги или перенаправляющие на сайт конкурентов

Такие ситуации могут быть особенно сложными для законопослушных компаний, потому что существование мошеннического сайта обнаруживается только тогда, когда ставший жертвой кибersквоттеров потребитель оставляет жалобу. Злоумышленники регистрируют доменное имя, которое содержит название чужой

компании и термин, описывающий ее товары или услуги. Такой сайт может появиться в результатах поисковиков, когда пользователь использует определенные ключевые слова. Перейдя на целевую страницу, потребитель перенаправляется на другой сайт кибersквоттеров или видит рекламные объявления и мошеннические предложения об услугах. Все это приносит злоумышленникам доход. Иногда кибersквоттеры регистрируют название торговой марки существующей компании, но используют другой общий домен верхнего уровня (например, .review, .loan, .shoe и т. д.).

Вывод

К сожалению, случаи кибersквоттинга очень сложно предотвращать и расследовать. Как показывают приведенные в статье примеры, кибберсквотеры используют множество тактик и постоянно совершенствуют стратегии, позволяющие избежать идентификации. Преступники часто используют сразу несколько сайтов, и потеря одного из них не наносит кибersквоттеру серьезного ущерба. Вместо одной уничтоженной веб-страницы мошенников тут же возникают еще несколько, и в результате компании вынуждены увеличивать расходы на борьбу с кибersквоттерами. Проблема усугубляется тем, что в распоряжении тайпсквоттеров сотни тысяч возможных опечаток и более 1000 общих доменов верхнего уровня, а это значит, что законопослушные компании не могут предусмотреть и превентивно зарегистрировать все доменные имена, чтобы помещать мошенникам. Однако мы все же рекомендуем заранее зарегистрировать варианты доменных имен компании с самыми распространенными опечатками. Кибersквоттеры постоянно совершенствуют свои методы, поэтому и компаниям следует неустанно оптимизировать процесс поиска и борьбы с сайтами мошенников.

Специалисты Osha Liang по товарным знакам и защите доменных имен имеют большой опыт успешного и экономически эффективного решения проблем киберсквоттинга, описанных в данной статье. Если вам нужна помощь в решении связанной с киберсквоттингом проблемы, свяжитесь с нами без колебаний.