УДК 343.985.7

С. М. Голятина
преподаватель кафедры криминалистики
учебно-научного комплекса по предварительному следствию
в органах внутренних дел
Волгоградской академии МВД России,
кандидат юридических наук

ТАРГЕТИРОВАННОЕ МОШЕННИЧЕСТВО: ПОНЯТИЕ И ПРОБЛЕМЫ РАССЛЕДОВАНИЯ

Зигмунд Фрейд писал: «Мы живем в очень странное время и с удивлением отмечаем, что прогресс идет в ногу с варварством» [1]. Применительно к настоящему дню скажем: варварство идет в ногу с прогрессом. Постепенная информатизация мира привела к появлению нового вида злоумышленников — киберпреступников, которые активно используют для достижения своих криминальных целей сеть Интернет, средства коммуникации, электронные платежные системы и т. д. Полагаем, что сегодня нет ни одного человека, который бы не слышал об интернет- и телефонном мошенничестве. Ущерб от него составляет несколько миллиардов рублей в год, о необходимости борьбы с ним говорят на самом высоком уровне, однако количество зарегистрированных сообщений о совершении таких преступлений увеличивается, а число раскрытых и расследованных преступлений растет довольно медленно. Так, член экспертного совета по экономике в Государственной думе Федерального собрания Российской Федерации А. Микаелов подчеркивает: «Производство по уголовным делам… в 75 % случаев приостанавливают за неустановлением обвиняемого, примерно 6 % уголовных дел прекращают по реабилитирующим основаниям и только 7 % уголовных дел направляют с обвинительным заключением в суд для дальнейшего разбирательства» [2]. В настоящее время особую тревогу вызывает так называемое таргетированное мошенничество, в основе которого лежит уникальная ссылка, сгенерированная для конкретного пользователя с учетом его потребностей и интересов. По словам специалистов компании Group-IB, в 2021 г. факты совершения такого мошенничества зафиксированы в 90 странах, в качестве приманки преступники нелегально эксплуатируют более 120 мировых брендов, а ущерб от действий злоумышленников составил 80 млн долларов (5,9 млрд руб.) ежемесячно [3]. В 2022 г. активность мошенников еще более возросла: так, в России только за первое полугодие количество мошенничеств с использованием таргета увеличилось на 579 %, а средняя сумма списания денежных средств с банковской карты составила 50 тыс. руб. [4]. Все сказанное обусловливает актуальность выбранной темы.

Таргетингом или таргетом называется механизм маркетинга, который позволяет из всех пользователей информационно-телекоммуникационной сети Интернет выделить по определенным параметрам целевую аудиторию и рекламировать ей свой товар для достижения максимального эффекта от рекламной компании [5], иными словами, это распространение информации о тех или иных продуктах, услугах, ориентированное на конкретного клиента.

Стремительное развитие таргетинг получил с появлением социальных сетей. Благодаря тому, что на страницах пользователи указывают даты рождения, города проживания, обозначают круг своих интересов, им можно показать соответствующую рекламу: кафе для празднования дня рождения, платные курсы по той или иной специальности, концерты и конференции, которые проходят в городе, и др. [6]. Здесь нужно остановиться подробнее и отметить, что нередко таргетированную рекламу не дифференцируют от контекстной, хотя разница между ними есть. Первая представляет собой объявления именно в социальных сетях. Ее настраивают на пользователей с конкретными параметрами: пол, возраст, образование, предпочтения и т. д., т. е. таргет основывается на данных пользователей. Вторая — это реклама в поисковых системах Яндекс, Google и на их партнерских сайтах. С ее помощью запущенные объявления демонстрируются после того, как пользователь ввел определенный запрос, т. е. контекстная реклама базируется на ключевых словах [7].

Основу работы таргета составляют четыре важнейших этапа: сбор информации о пользователях с помощью cookie; проведение анализа данных и выделение целевой аудитории, которая может проявить интерес к тому или иному товару; автоматическая запись информации, формирование графиков и диаграмм в целях удобства мониторинга данных; создание и размещение объявления с учетом специфики целевой аудитории и частоты посещаемости сайтов [5].

Каким образом это работает? Например, в популярной социальной сети «ВКонтакте», аудитория которой насчитывает в настоящее время только в России 53,6 млн человек, вы хотите запустить рекламу розничного офлайн-магазина товаров для творчества и рукоделия. Для начала необходимо задать правильные настройки. Во-первых, следует определиться с местоположением, чтобы не платить за показ рекламы жителям тех населенных пунктов, где вашего магазина попросту нет. Во-вторых, объявление стоит демонстрировать только тем людям, которым интересна данная тема: художникам, дизайнерам, швеям, педагогам, тем, кто увлекается вышивкой, вязанием, скрапбукингом, квиллингом и т. д. Для этого и нужен таргетинг, с помощью которого вы исключаете показы рекламы нецелевой аудитории. Здесь необходимо упомянуть такой термин, как парсинг — процесс сбора и систематизации информации о пользователях посредством парсеров — сервисов, получающих данные из открытых источников и

помогающих таргетологам находить и анализировать целевую аудиторию: «С помощью парсера можно найти родителей по возрасту детей, найти мужей, чьи жены празднуют через три дня день рождения… Найти тех, кто разместил нужные вам аудио или отреагировал на промо-пост… проанализировать посты или вовлеченность сообщества… Также есть разные фильтры для сортировки сообществ или пользователей по интересам, вероисповеданию, количеству контента…» [8].

Таким образом, таргетинг является своего рода персональным предложением — разновидностью маркетингового сотрудничества с потребителем в режиме один на один, побуждающим клиента к приобретению товара или услуги на основе его предпочтений. С точки зрения психологии продаж человек скорее обратит внимание на ту продукцию, которая в наибольшей степени соответствует его потребностям и желаниям, а эффективная коммуникации строится тогда, когда собеседник (в нашем случае клиент) чувствует свою исключительность, участливое отношение к себе и своим интересам. Именно на избранности, эксклюзивности — важнейших триггерах маркетинга — строится таргетированное мошенничество. Злоумышленники рассчитывают, что потенциальная жертва обратит внимание на яркое маркетинговое предложение. Обычно оно начинается такими фразами, как: «Только для вас сегодня на особых условиях мы предлагаем…» или «Уважаемый клиент! Поздравляем! Вы один из 100 отобранных пользователей, которым выпал уникальный шанс выиграть…». Как правило, за подобными сообщениями следует опрос клиента, в результате прохождения которого он теряет свои деньги.

Мошеннические схемы с опросами и выигрышами не являются новинкой. Но если в прошлом они развивались за счет массовости, то в настоящее время стали более технологичными и персонализированными. Сегодня под жертву создается отдельная таргетированная ссылка. В ее основе лежит своеобразный «отпечаток» пользователя (страна, часовой пояс, язык, тип браузера, IP и т. д.). Важно то, что данная ссылка открывается только у потенциального потерпевшего, другие лица без необходимых cookie-файлов перейти по ней не смогут. При этом даже если пользователь распознает обман и отправит ссылку на блокировку, она не сможет быть заблокирована. Обычно такая ссылка ведет на страницу с фейковым опросом от имени известного бренда (в настоящее время злоумышленники эксплуатируют более 120 мировых брендов главным образом из отраслей телекоммуникации, e-commerce и ритейла), за прохождение которого обещана награда. После этого пользователю предлагается заполнить форму с персональными данными (фамилия, имя, отчество, адрес электронной почты, номер телефона, номер банковской карты со сроком ее действия, cvv). Получив их, мошенники могут распоряжаться ими как угодно (совершать

покупки, продавать данные в даркнете и т. д.). Однако, прежде чем оказаться на странице с опросом, жертва, нажав на ссылку, попадает в так называемую клоаку трафика: трафик распределяется на «белый», который не несет в себе никакой опасности, «серый» и «черный». Два последних нарушают правила распространения рекламы и создают реальную угрозу кибербезопасности пользователя: здесь жертва несколько раз перенаправляется на разные страницы, которые собирают информацию о геолокации, языке, типе браузера и т. д. Именно на данной основе конструируется итоговая ссылка, которая и работает только один раз [9]. При этом такая ссылка может содержать вредоносное программное обеспечение, оформлять на жертву платные подписки и др. Подчеркнем, что таргетированные ссылки по сравнению со спамом в сети Интернет и СМС-сообщениях — это относительно новый вид онлайн-мошенничества, представляющий угрозу не только для пользователей, которые теряют свои денежные средства и персональные данные, но и для брендов, несущих финансовые и репутационные потери.

Обозначим круг основных проблем, с которыми сталкиваются сотрудники правоохранительных органов при раскрытии и расследовании таргетированного мошенничества. Большинство из них являются такими же, что и при расследовании фактов любого мошенничества, совершенного бесконтактным способом посредством информационно-телекоммуникационной сети Интернет. Однако некоторые все же имеют свою специфику. Во-первых, важно отметить, что таргетированные ссылки, созданные мошенниками, далеко не всегда могут распознать даже специальные программы. Кроме того, с момента появления данные ссылки значительно изменили свой вид. Сегодня в большинстве из них отсутствует референер (информация о том, с какого сайта пришел пользователь), т. е. они стали менее информативными для анализа. Во-вторых, если программе удается заблокировать такую ссылку, на ее месте появляются сразу же несколько новых, поэтому данную схему мошенничества довольно трудно устранить. В-третьих, в значительной части случаев таргетированное мошенничество совершает не один человек, за такими преступлениями, как правило, стоит преступное сообщество, ибо это весьма прибыльный «бизнес».

Ранее мы уже неоднократно отмечали иные проблемы, сопровождающие расследование интернет-краж и мошенничеств [10]. В полной мере это относится и к таргетированному мошенничеству. Прежде всего, здесь необходимо говорить о недостаточном уровне компетенции сотрудников органов внутренних дел и небольшом опыте их работы со специфическими источниками доказательственной информации, находящейся в электронной среде в виде электронных сообщений, страниц, сайтов. Кроме того, большинство сотрудников правоохранительных органов имеют традиционное юридическое образование, которое ориентировано на решение правовых проблем и не предполагает связи

с техническими науками, без чего невозможно понимание механизма совершения киберпреступления, в том числе таргетированного мошенничества, и его эффективное расследование. Следующая проблема связана с назначением судебных компьютерных экспертиз. Стоит подчеркнуть, что сегодня в экспертно-криминалистических центрах Министерства внутренних дел России имеется недостаточное количество экспертов, имеющих допуск к их производству. Само же производство характеризуется длительностью, а также высокой стоимостью исследования при его назначении в негосударственные судебно-экспертные учреждения.

В завершение сделаем несколько выводов:

− Таргетингом называется механизм продаж, основанный на демонстрации рекламы целевой аудитории. Таргетированные объявления базируются на данных пользователей социальных сетей, что отличает их от контекстных.

− Принцип работы таргетированной ссылки состоит в следующем: пользователь, нажав на интересующее его объявление, оказывается в так называемой клоаке трафика, где перенаправляется с одной страницы на другую. На этих страницах осуществляется сбор информации о стране пользователя, его языке, типе браузера и т. д. На основе полученных сведений создается уникальная ссылка, работающая только у этого пользователя. Обычно она ведет на страницу с фейковым опросом от имени известного бренда, за прохождение которого обещана награда. После этого пользователю предлагается заполнить форму с персональными данными (фамилия, имя, отчество, адрес электронной почты, номер телефона, номер банковской карты со сроком ее действия, cvv). Получив их, мошенники могут распоряжаться ими по своему усмотрению.

− Круг основных проблем, сопровождающих расследование таргетированного мошенничества, составляют: недостаточной уровень компетенции сотрудников органов внутренних дел и небольшой опыт их работы со специфическими источниками доказательственной информации, находящейся в электронной среде; недостаток лиц, производящих судебные компьютерные экспертизы в экспертно-криминалистических центрах Министерства внутренних дел России, высокая стоимость таких экспертиз в негосударственных учреждениях; постоянное видоизменение и совершенствование структуры самой таргетированной ссылки; трудности ее обнаружения даже специальными программами.

1. Зигмунд Фрейд [Электронный ресурс] // Проза.ру. URL: https://proza.ru/2012/10/28/205 (дата обращения: 06.10.2022). Перейти к источнику Вернуться к статье

2. Немцева М. «Их слишком много»: почему киберпреступления остаются нераскрытыми [Электронный ресурс] // Известия. URL: https://iz-

ru.turbopages.org/iz.ru/s/1166840/mariia-nemtceva/ikh-slishkom-mnogo-pochemu-kiberprestupleniia-ostaiutsia-neraskrytymi (дата обращения: 06.10.2022). Перейти к источнику Вернуться к статье

3. Агапов В. Специалисты подсчитали заработок мошенников на акциях «только для вас» [Электронный ресурс] // Секрет Фирмы. URL: https://secretmag-ru.turbopages.org/turbo/secretmag.ru/s/news/specialisty-podschitali-zarabotok-moshennikov-na-akciyakh-tolko-dlya-vas-21-12-2021.htm (дата обращения: 14.11.2022). Перейти к источнику Вернуться к статье

4. Мошенники воспользовались вибрацией брендов [Электронный ресурс] // ComNews.ru. URL: https://www.comnews.ru/content/221951/2022-08-31/2022-w35/moshenniki-vospolzovalis-vibraciey-brendov (дата обращения: 14.11.2022). Перейти к источнику Вернуться к статье

5. Таргетинг [Электронный ресурс]. URL: https://rtb.sape.ru/content/glossary/%D1%82-rus/targeting/ (дата обращения: 14.11.2022). Перейти к источнику Вернуться к статье

6. Когда впервые появилась таргетированная реклама? [Электронный ресурс]. URL: https://yandex.ru/q/question/kogda_vpervye_poiavilas_targetirovannaia_b89ea886/ (дата обращения: 14.11.2022). Перейти к источнику Вернуться к статье

7. Шпак А. Таргетированная реклама: полный гайд для новичков [Электронный ресурс] // TexTerra. URL: https://texterra.ru/blog/chto-takoe-targetirovannaya-reklama-polnyy-gayd-dlya-novichkov.html (дата обращения: 14.11.2022). Перейти к источнику Вернуться к статье

8. Канарская Л. Как не слить бюджет на таргете в ВК — 8 проверенных парсеров [Электронный ресурс] // TexTerra. URL: https://texterra.ru/blog/kak-sekonomit-na-targetirovannoy-reklame-v-vk-s-pomoshchyu-parsera.html (дата обращения: 14.11.2022). Перейти к источнику Вернуться к статье

9. Кравцов Я., Егоров Е. Только для вас. Как работает таргетированное мошенничество [Электронный ресурс]. URL: https://blog.group-ib.ru/target (дата доступа: 16.11.2022). Перейти к источнику Вернуться к статье

10. Голятина С. М. Методика расследования хищений электронных денежных средств : дис. … канд. юрид. наук : 12.00.12. Волгоград, 2022. 196 с. Вернуться к статье