НОВАЯ МНОГОСТУПЕНЧАТАЯ СХЕМА МОШЕНИЧЕСТВА «КРОЛИЧЬЯ НОРА»

ROOT LEVEL RESOURCES

«Как и Алису, бегущую за белым кроликом в сказке Льюиса Кэрролла, злоумышленники ведут своих жертв с ресурса на ресурс, похищая персональную информацию, данные банковских карт или деньги»

специалисты Group-IB

Классический фишинг стал менее эффективным. Пользователи уже не доверяют спонтанным сообщениям о выигрыше или вознаграждении. Кто-то еще может по глупости или невнимательности повестись на нее, но в целом такой фишинг уже никого не пугает. Интернет-пользователи и бренды расслабились и это сподвигло мошенников придумать новую схему фишинга. Все как в фильмах про апокалипсис, вирус мутировал, стал устойчивее, и прежние методы лечения ему — как слону дробина.

Новая схема условно названа по аналогии со сказкой «Алиса в Стране чудес», поскольку начинается с безобидных шагов, в результате которых пользователь доверяет «белому кролику», теряет бдительность и попадает в «кроличью нору».

Опасность в том, что каждый этап этой схемы не кажется подозрительным службам безопасности, атаки учитывают индивидуальные характеристики жертвы, а пользователи склонны самостоятельно пройти по длинной цепочке вслед за «белым кроликом».

Потенциальными жертвами такой схемы в основном становятся доверчивые подростки, которые пользуются картами родителей. Также злоумышленники под предлогом социальных экспериментов, краудфандинга или благотворительных акций в соцсетях с легкостью могут завоевать доверие молодых людей, активно участвующих в таких мероприятиях.

Условно всю мошенническую схему специалисты Group-IB делят на две большие части:

Часть 1: «Следуй за белым кроликом»

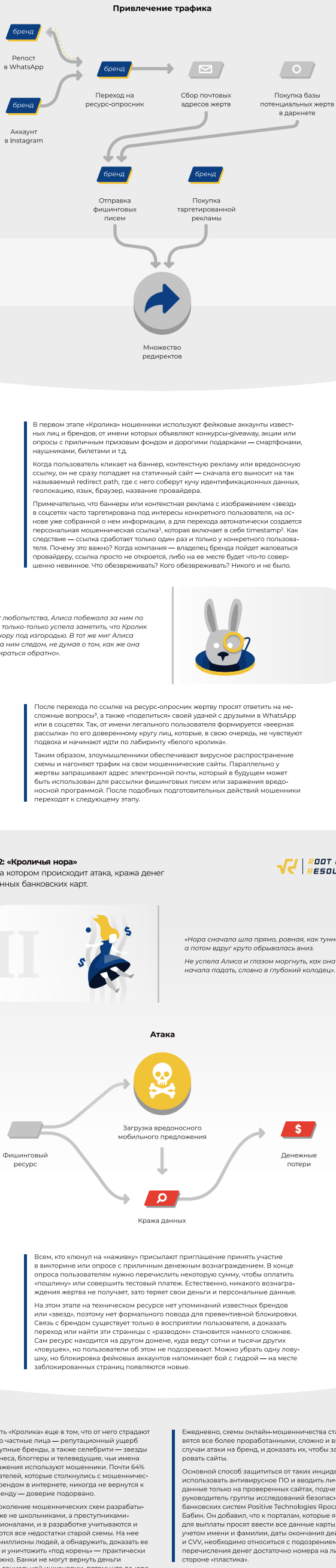
Этап, на котором происходит привлечение трафика

ROOT LEVEL RESOURCES

«Алисе наскучило сидеть с сестрой без дела на берегу реки; разок-другой она заглянула в книжку, которую читала сестра, но там не было ни картинок, ни разговоров. Вдруг мимо пробежал белый кролик с красными глазами, который на бегу говорил: «Ах, боже мой, боже мой! Я опаздываю».

Раньше Алиса никогда не видела кролика с часами, да еще с жилетным карманом в придачу!»

Привлечение трафика



В первом этапе «Кролика» мошенники используют фейковые аккаунты известных лиц и брендов, от имени которых объявляют конкурсы-giveaway, акции или опросы с приличным призовым фондом и дорогими подарками — смартфонами, наушниками, билетами и т.д.

Когда пользователь кликает на баннер, контекстную рекламу или вредоносную ссылку, он не сразу попадает на статичный сайт — сначала его выносит на так называемый redirect path, где с него соберут кучу идентификационных данных, геолокацию, язык, браузер, название провайдера.

Примечательно, что баннеры или контекстная реклама с изображением «звезд» в соцсетях часто таргетирована под интересы конкретного пользователя, на основе уже собранной о нем информации, а для перехода автоматически создается персональная мошенническая ссылка[1], которая включает в себя timestamp[2]. Как следствие — ссылка сработает только один раз и только у конкретного пользователя. Почему это важно? Когда компания — владелец бренда пойдет жаловаться провайдеру, ссылка просто не откроется, либо на ее месте будет что-то совершенно невинное. Что обезвреживать? Кого обезвреживать? Никого и не было.

«Сгорая от любопытства, Алиса побежала за ним по полю. Она только-только успела заметить, что Кролик юркнул в нору под изгородью. В тот же миг Алиса юркнула за ним следом, не думая о том, как же она будет выбираться обратно».

После перехода по ссылке на ресурс-опросник жертву просят ответить на несложные вопросы[3], а также «поделиться» своей удачей с друзьями в WhatsApp или в соцсетях. Так, от имени легального пользователя формируется «веерная рассылка» по его доверенному кругу лиц, которые, в свою очередь, не чувствуют подвоха и начинают идти по лабиринту «белого кролика».

Таким образом, злоумышленники обеспечивают вирусное распространение схемы и загоняют трафик на свои мошеннические сайты. Параллельно у жертвы запрашивают адрес электронной почты, который в будущем может быть использован для рассылки фишинговых писем или заражения вредоносной программой. После подобных подготовительных действий мошенники переходят к следующему этапу.

Часть 2: «Кроличья нора»

Этап, на котором происходит атака, кража денег или данных банковских карт.

ROOT LEVEL RESOURCES

«Нора сначала шла прямо, ровная, как туннель, а потом вдруг круто обрывалась вниз.

Не успела Алиса и глазом моргнуть, как она начала падать, словно в глубокий колодец».

Атака

Всем, кто клюнул на «наживку» присылают приглашение принять участие в викторине или опросе с приличным денежным вознаграждением. В конце опроса пользователям нужно перечислить некоторую сумму, чтобы оплатить «пошлину» или совершить тестовый платеж. Естественно, никакого вознаграждения жертва не получает, зато теряет свои деньги и персональные данные.

На этом этапе на техническом ресурсе нет упоминаний известных брендов или «звезд», поэтому нет формального повода для превентивной блокировки. Связь с брендом существует только в восприятии пользователя, а доказать переход или найти эти страницы с «разводом» становится намного сложнее. Сам ресурс находится на другом домене, куда ведут сотни и тысячи других «ловушек», но пользователи об этом не подозревают. Можно убрать одну ловушку, но блокировка фейковых аккаунтов напоминает бой с гидрой — на месте заблокированных страниц появляются новые.

Опасность «Кролика» еще в том, что от него страдают не только частные лица — репутационный ущерб несут крупные бренды, а также селебрити — звезды шоу-бизнеса, блоггеры и телеведущие, чьи имена и изображения используют мошенники. Почти 64% пользователей, которые столкнулись с мошенничеством с брендом в интернете, никогда не вернутся к этому бренду — доверие подорвано.

Новое поколение мошеннических схем разрабатывается уже не школьниками, а преступниками-профессионалами, и в разработке учитываются и устраняются все недостатки старой схемы. На нее ведутся миллионы людей, а обнаружить, доказать ее наличие и уничтожить «под корень» — практически невозможно. Банки не могут вернуть деньги жертвам социальной инженерии, потому что де-юре пользователь сделал перевод на счет мошенника или поделился данными своей карты добровольно.

Ежедневно, схемы онлайн-мошенничества становятся все более проработанными, сложно и выявить случаи атаки на бренд, и доказать их, чтобы заблокировать сайты.

Основной способ защититься от таких инцидентов — использовать антивирусное ПО и вводить личные данные только на проверенных сайтах, подчеркнул руководитель группы исследований безопасности банковских систем Positive Technologies Ярослав Бабин. Он добавил, что к порталам, которые якобы для выплаты просят ввести все данные карты, с учетом имени и фамилии, даты окончания действия и CVV, необходимо относиться с подозрением: для перечисления денег достаточно номера на лицевой стороне «пластика».

ROOT LEVEL RESOURCES

Будьте бдительны!
Безопасность зависит от нас самих!

***1** – Ссылка генерируется под конкретного пользователя, исходя из его местоположения, IP-адреса, модели устройства, user-агента. Эксперты Group-IB утверждают, что мошенники в соцсетях узнают всю информацию о жертве из ее открытого аккаунта, что повышает вероятность успешной аферы.*

***2** – Данные о конкретной дате и времени*

***3** – Психологическая ловушка, позволяющая завоевать доверие*