Безопасность

ЗАМАНЧИВАЯ ОХОТА «ТРОЯНЦЕВ»

Дмитрий КУДРЕВИЧ,
представитель Kaspersky в Беларуси

Мобильные банковские «троянцы» – одна из наиболее распространенных и опасных мобильных угроз. Злоумышленники используют их для охоты за финансовыми данными, которые могут относиться к системам онлайн-банкинга и электронных платежей.

Например, за 2022 год решения Kaspersky обнаружили почти 200 тысяч новых загрузчиков мобильных банковских троянцев, что вдвое больше, чем в 2021 году. Столь резкий рост числа подобных зловредов наблюдается впервые за шесть лет. Всего за минувший год выявлено более 1,6 млн вредоносных программ или установщиков нежелательного ПО. Об этом говорится в отчете Kaspersky «Мобильные угрозы в 2022 году».

Атакующие часто распространяют Trojan Banker как через неофициальные, так и официальные магазины приложений. В Google Play до сих пор есть загрузчики семейств банковских троянцев, таких как Sharkbot, Anatsa/Teaban, Octo/Coper и Xenomorph, замаскированные под якобы полезные программы.

В 2022 году защитные решения компании Kaspersky заблокировали почти 1,7 млн попыток пользователей в Беларуси перейти на фишинговые ресурсы с домашних устройств. Это позволяет злоумышленникам угонять аккаунты, собирать конфиденциальные данные и красть данные банковских карт. Фишинг, нацеленный на пользователей социальных сетей, опасен тем, что мошенники могут получить доступ не только к самой платформе, но и к привязанным к ней сервисам.

Фишинговые атаки* часто нацелены и на компании. Так, в Беларуси в 2022 году было заблокировано более 825 тыс. попыток перехода корпоративных пользователей по подозрительным ссылкам из писем. При этом, помимо обычных схем атакующих, состоящих из одного этапа, в прошлом году появились многоэтапные атаки: в первом письме мошенники от лица потенциального клиента просят уточнить информацию о товарах и услугах. Если жертва отвечает на такое письмо, злоумышленники переходят непосредственно к фишинговой атаке, используя при этом методы социальной инженерии.

В Беларуси в минувшем году решения Kaspersky заблокировали почти 320 тыс. попыток перейти на скам-ресурсы. Популярной приманкой были «акции» якобы от имени крупных банков. Посетителю фальшивой страницы предлагали получить единовременную помощь или за вознаграждение пройти

* Фишинговые атаки – это рассылка мошеннических сообщений, источник которых кажется надежным. Как правило, для этого используется электронная почта. Цель злоумышленников заключается в краже конфиденциальной информации (например, данных кредитной карты и учетных данных) или установке на устройство жертвы вредоносного ПО.

опрос для улучшения качества обслуживания. При этом злоумышленники использовали множество различных приемов, чтобы усыпить бдительность жертвы: логотипы компаний; уверения в том, что все акции официальны и не являются мошенничеством; детальное описание предложения, делающее его очень похожим на настоящее. Все это приметы скама – одной из популярных разновидностей фишинга.

Фишинг не сдает своих позиций и продолжает оставаться актуальной угрозой как для домашних, так и для корпоративных пользователей. При этом мы ожидаем, что в 2023 году появятся новые уловки, нацеленные на бизнес, ведь такие атаки, как правило, приносят злоумышленникам значительную прибыль.

Атакующие часто маскируют вредоносные рассылки под деловые письма, поэтому компаниям стоит позаботиться о повышении цифровой грамотности своих сотрудников. Осведомленность об угрозах подобного рода позволит существенно минимизировать риски.

Для защиты от киберугроз Kaspersky рекомендует придерживаться следующих правил:

- не переходить по сомнительным ссылкам из писем, сообщений в мессенджерах или СМС;
- регулярно устанавливать обновления операционной системы и приложений;
- загружать приложения только из официальных магазинов;
- использовать сложные и разные пароли для учетных записей;
- не давать приложениям доступ к тем функциям, которые им не нужны;
- установить надежное защитное решение, которое предупредит о потенциально опасном сайте, такое как Kaspersky Internet Security.