Преступники соорудили самодельную антенну для масштабной кампании, но где-то просчитались…

Британским правоохранителям удалось раскрыть беспрецедентную схему интернет-мошенничества, в рамках которой злоумышленники использовали самодельную телефонную вышку для массовой фишинговой операции. Двое подозреваемых уже арестованы.

По данным полиции Сити Лондона, изъятая вышка представляла собой самодельную мобильную антенну, получившую кодовое название «СМС-пушка» . Это первое в Великобритании устройство такого рода, специально сконструированное для распространения огромных партий вредоносных материалов. При этом злоумышленники каким-то образом обходили системы защиты операторов от СМС-Фишинг (phishing) – это метод мошенничества, когда злоумышленник пытается получить доступ к личной информации, такой как пароли, номера банковских карт и другие конфиденциальные данные, путем подделки электронных сообщений, сайтов, приложений и других форм интернет-коммуникации." data-html="true" data-original-title="Фишинг" >фишинга или «смишинга».

Преступники выдавали себя за банки, госструктуры и прочие официальные организации. Под (казалось бы) надежным прикрытием они пытались выманить у получателей личные данные, пароли и платежные реквизиты.

«Киберпреступники придумывают все более изощренные схемы, применяя сложные уловки для обмана граждан и хищения ценностей, — прокомментировал ситуацию временный руководитель подразделения по киберпреступлениям Дэвид Винт. — Крайне важно объединить усилия с партнерами, чтобы не допустить новых случаев мошенничества».

Винт напомнил, что ни банки, ни госорганы никогда не запрашивают у клиентов конфиденциальную информацию по СМС или телефону: «Если вы получили подозрительное сообщение, сообщите о нем, переслав его на номер 7726».

Большинство британских операторов участвуют в системе, позволяющей абонентам пересылать спам-сообщения на этот номер для проверки. После этого провайдеры могут блокировать отправителя. К примеру, местный оператор EE уже заблокировал десятки миллионов мошеннических СМС после усиления антиспам-фильтров в 2021 году. Более того, в розничных салонах EE новые клиенты могут подтвердить свою личность, что минимизирует риск отправки спама с их учетных записей.

32-летний Хуайонг Сюй из Кройдона был арестован 23 мая по обвинению в хранении дополнительной инфраструктуры для мошеннических кампаний. Ему предстоит предстать перед судом 26 июня. Второй задержанный был арестован 9 мая в Манчестере, но позднее отпущен под залог. Личность этого человека не раскрывается.

Расследование ведется совместно с операторами связи, регулятором Ofcom и Национальным центром кибербезопасности. В Ofcom подчеркнули, что телефонное мошенничество наносит серьезный ущерб жертвам, поэтому регулятор тесно взаимодействует с правоохранителями и остальными представителями отрасли для решения проблемы.

По неподтвержденным данным, СМС-пушки могут представлять собой IMSI-перехватчики — устройства для тайной перехвата трафика сотовой связи, обычно используемые спецслужбами. В руках злоумышленников они способны взламывать защитные механизмы телефонов и обходить антиспам-фильтры для рассылки фишинга. Однако официального подтверждения этой версии пока нет.

В прошлые годы США неоднократно подвергались критике за злоупотребление IMSI-перехватчиками и их использование с нарушением федеральных норм. В 2017 году британские власти пытались задействовать эти устройства для блокировки связи в тюрьмах. Однако заключенные быстро заподозрили неладное, когда заметили, что обертывание устройств фольгой блокирует работу перехватчиков. Представители правоохранительных органов вынуждены были признать провал испытаний.