До 100 000 мошеннических сообщений рассылается ежедневно.

Пакистанские пользователи банков стали мишенью новой фишинговой кампании группы «Smishing Triad». Киберпреступники отправляют поддельные сообщения от имени Pakistan Post, пытаясь украсть личную и финансовую информацию. Обнаружить данную вредоносную активность удалось экспертам из Resecurity – это компания, которая занимается информационной безопасностью. Она предоставляет решения для защиты от цифровых угроз и кибератак, а также помогает компаниям и организациям сохранять конфиденциальность информации. Компания предлагают ряд услуг, таких как мониторинг угроз, обнаружение инцидентов, анализ и реагирование на киберугрозы." data-html="true" data-original-title="Resecurity" >Resecurity.

Сам по себе Смишинг или СМС-фишинг – это мошенническая техника, при которой злоумышленники используют простые текстовые сообщения для обмана людей и получения доступа к их личным данным или финансовым счетам.

 Обычно злоумышленники отправляют сообщения, которые выглядят как официальные сообщения от известных компаний или организаций, таких как банки, поставщики услуг связи или онлайн-магазины. В этих сообщениях могут содержаться ссылки на вредоносные сайты или просьбы предоставить личную информацию, такую как пароли, номера кредитных карт или номера социального страхования." data-html="true" data-original-title="Смишинг" >смишинг представляет собой комбинацию СМС-сообщений и фишинга, используемую, чтобы обманом вынудить жертв раскрыть конфиденциальные данные. В рассмотренном киберспециалистами случае злоумышленники выдавали себя за Pakistan Post, используя местные телефонные номера для создания иллюзии подлинности, требуя оплату и данные кредитных карт для покрытия дополнительных сборов.

В отчёте Resecurity упоминается, что ранее «Smishing Triad» уже атаковала онлайн-банкинг, электронную коммерцию и платёжные системы в США, ЕС, ОАЭ и Саудовской Аравии, а теперь нацелилась и на Пакистан. Тактика «Smishing Triad» остаётся неизменной: они выдают себя за доверенную организацию, создают чувство срочности и похищают ценную информацию.

Группировка базируется в Китае и использует смишинг в качестве основного метода атаки. В сентябре 2023 года они подделывали сообщения от ведущих почтовых и логистических служб по всему миру, включая USPS, Correos, New Zealand Post и The Royal Mail. А в декабре притворялись госслужащими из Объединённых Арабских Эмиратов. В этом году активность группы началась в мае и достигла пика в июне.

Сообщения отправляются через iMessage и SMS, привлекая получателей сообщениями о недоставленных посылках от TCS, Leopard, FedEx и других курьерских компаний, либо о срочных проблемах с аккаунтами. Ежедневно отправляется от 50 000 до 100 000 сообщений, использующих украденные базы данных из даркнета, содержащие информацию граждан, включая номера телефонов.

Пользователи мобильных операторов в Пакистане, таких как Jazz/Warid, Zong, Telenor Pakistan и Ufone на платформе Reddit подтвердили получение подобных фишинговых сообщений.

Наиболее активные смишинговые наборы обнаружены на хостах «pk-post-goi.xyz» и «ep-gov-ppk.cyou», созданных злоумышленником, имитирующим Express Mail Track & Trace System.

Большинство доменов были зарегистрированы через сервис NameSilo с использованием анонимных данных и фальшивых контактных сведений, которые экспертам Resecurity удалось успешно ликвидировать.

Также злоумышленники использовали сервисы сокращения URL и генерации QR-кодов для обхода обнаружения, включая платформы QR Code Generator, IS[.]GD, 2h[.]ae и Linkr[.]it.

Национальная команда по реагированию на киберчрезвычайные ситуации Пакистана (PKCERT) выпустила консультативное предупреждение, призывая граждан к проактивным мерам защиты от подобного рода мошенничества.

Телекоммуникационные операторы Пакистана также предупреждены о необходимости улучшения систем обнаружения мошенничества и блокировки вредоносной активности.

Для защиты от атак местным жителям рекомендуется проявлять скептицизм, игнорировать подозрительные сообщения, избегать перехода по сомнительным ссылкам, использовать антивирусное ПО и сообщать о любых попытках мошенничества своему мобильному оператору.