Как мошенники «сотрудничают» с провайдерами и эксплуатируют легальные сервисы.

Группа исследователей из Университета Северной Каролины подробно изучила механизмы СМС-фишинга . Их работа проливает свет как на общие масштабы проблемы, так и на внутреннюю структуру преступных фишинговых операций по всему миру.

Согласно отчету организации Anti-Phishing Working Group , в 2023 году количество фишинговых атак подобного рода достигло невиданных ранее высот. При 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" >фишинге злоумышленники рассылают поддельные сообщения, маскируясь под надежные организации — банки, госструктуры и т.д. Их цель — выманить у жертв конфиденциальные данные, включая логины, пароли и реквизиты банковских карт, обманным путем.

До недавнего времени исследователи располагали крайне скудной информацией о работе фишинговых группировок. Провайдеры опасались нарушить приватность абонентов при анализе СМС-трафика и неохотно помогали в расследованиях. Чтобы преодолеть это препятствие, специалисты прибегли к использованию СМС-шлюзов — онлайн-сервисов для получения виртуальных одноразовых номеров телефонов.

Заполучив более 2000 таких «приманок», команда во главе с аспирантом Алексом Нахапетяном стала ждать, когда на них начнут поступать мошеннические послания. За 396 дней мониторинга они зафиксировали 67 991 фишинговое СМС. Их можно разделить на 35 128 уникальных кампаний с практически идентичным содержанием. Дальнейший анализ позволил связать эти кампании с 600 отдельными преступными операциями.

Результаты исследования оказались крайне любопытными. Выяснилось, что для реализации своих противоправных схем фишеры широко используют ту же легальную веб-инфраструктуру и публичные облачные сервисы, что и добропорядочные организации. Речь идет о мейнстримных хостингах, сервисах сокращения ссылок, «облаках» и прочем.

Подтверждением служат и некоторые детали в тексте самих СМС. Так, в конце многих сообщений содержатся пометки вроде «маршрут 7» или «маршрут 9».

Предположительно, эти метки используются мошенниками для тестирования различных путей доставки сообщений и выявления наиболее эффективных стратегий.

Ученые также обнаружили, что некоторые фишеры не просто пользуются общедоступной инфраструктурой, но и создают собственную. К примеру, отдельные группировки регистрируют уникальные доменные имена исключительно для размещения на них своих «частных» сервисов сокращения ссылок. По мнению экспертов, такой подход может использоваться для обеспечения дополнительной защиты преступных операций или даже указывать на существование черного рынка таких услуг.

Специалисты также решили проверить, насколько хорошо провайдеры и их клиенты защищены от подобных угроз, и сложно ли фишерам добиваться своих целей. Они разослали безвредные фишинговые СМС на 10 номеров напрямую со своих устройств и через популярный сервис массовой рассылки Pavlok. Все сообщения были успешно доставлены получателям, однако затем учетная запись исследователей в Pavlok была заблокирована.

Впрочем, поиски показали, что имеются и другие сервисы для массовых СМС-рассылок, открыто рекламирующие свои услуги в интернете и не брезгующие сотрудничеством с преступниками.

В некоторых случаях удавалось перехватить сообщения, содержавшие вредоносные URL-адреса, до того, как злоумышленники успели полностью развернуть соответствующие поддельные веб-ресурсы. Вероятно, СМС отправлялись, чтобы проверить работоспособность ссылок перед запуском кампании в полном масштабе. Этот факт открывает возможность для выявления зарождающихся фишинговых атак на самых ранних стадиях путем постоянного сканирования и анализа трафика.

Исследование также проливает свет на экономику преступной индустрии СМС-фишинга. Оказалось, что новичкам в этом деле совсем несложно приобрести готовый к работе фишинговый комплект со всей необходимой инфраструктурой — программный код, домены, сервисы массовых рассылок и прочее. А если какой-то из ресурсов будет заблокирован, это не проблема — есть возможность оперативно переключиться на запасной из обширного преступного арсенала.

Результаты этой масштабной работы были представлены 20 мая на симпозиуме IEEE, посвященном вопросам безопасности и конфиденциальности, в Сан-Франциско. Соавторами исследования выступили аспирант Сатвик Прасад, бывший студент Кевин

Чайлдс, профессора Александрос Капрэвелос и Брэд Ривз, а также сотрудники PayPal Адам Уэст и Йеганех Ладвиг. Открытия ученых призваны помочь правоохранителям более эффективно противостоять растущей угрозе СМС-фишинга и защитить пользователей от утечек и финансовых потерь.