УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.144

ВРАЗЛИВОСТІ МЕСЕНДЖЕРІВ «TELEGRAM», «WHATSAP», «VIBER»

Пашнєва О.Р.
Науковий керівник – Євгеньєв А.М.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: olha.pashnieva@gmail.com

The proliferation of messaging applications such as Telegram, WhatsApp, and Viber has revolutionized communication, but it has also introduced a myriad of security concerns. This paper provides a analysis of the vulnerabilities present in the messengers Telegram, WhatsApp and Viber, with a particular focus on the threat of phishing attacks. As these platforms handle sensitive personal and professional information, they are increasingly becoming prime targets for attackers who seek to exploit unsuspecting users through deceptive tactics. The relevance of this research is due to the increasing use of these messengers for communication in various domains, including business, personal, and government.

У червні 2016-го року «International Journal of Electrical and Computer Engineering» було опубліковано роботу, що дослідила вже популярні на той час «Telegram», «Whatsap» та «Viber» за багатьма критеріями, щоб обрати серед них найбільш зручний і захищений [1]. Висновком стало: «Viber є найбільш функціональним месенджером, але якщо основною проблемою є безпека спілкування, то розумніше обрати Telegram. Telegram пропонує можливість синхронізації, надшвидкий сервіс, надійне резервне копіювання та кращі функції безпеки.» З плином часу й розвитком систем безпеки, нині всі найвідоміші месенджери використовуюсь двофакторну аутентифікацію та наскрізне шифрування. Це передбачає, що ключі дешифрування до чатів та дзвінків зберігаються лише на пристроях користувачів: повідомлення неможливо перехопити й прочитати, а розшифровуються вони тільки на пристроях співрозмовників. Будь-які інші особи, навіть співробітники месенджеру, не мають доступу до цих ключів, тому дзвінки та повідомлення можуть бути прочитані, чи прослухані лише учасниками діалогу.

Коли розшифрування перехопленого повідомлення стало невигідним, популярність отримали інші види атак [2]. Кіберзлочинці можуть маскуватися. Вони можуть зв'язатися із законним користувачем, видаючи себе за іншу фізичну або юридичну особу, щоб отримати конфіденційні дані (особисті дані, паролі, номери кредитних карток) або розгорнути шкідливе ПЗ (шкідливе програмне забезпечення, що отримує несанкціонований доступ до будь-якої системи). Атаки такого типу називають фішингом. За даними компанії Vesta,

що є платформою наскрізної гарантії транзакцій для онлайн-покупок, 2021 року фішингові схеми стали другою найімовірнішою причиною витоку даних і коштували підприємствам у середньому 4,65 мільйона доларів. Того самого року група аналізу загроз Google повідомила про блокування близько 800 мільйонів фішингових листів, пов'язаних із COVID-19, на день.

Соціальні мережі дали можливість кіберзлочинцям не тільки автоматизувати процес, використовуючи ботів для розсилки, але й для реклами різних послуг – від продажу наборів для фішингу до допомоги в налаштуванні користувацьких фішингових кампаній – усім, хто готовий платити. Крім того, не потрібно застосовувати великих зусиль, щоб знайти безкоштовний контент, або посібники, які шахраї так охоче поширюють серед своєї аудиторії Telegram. Це слугує своєрідною приманкою для менш досвідчених фішерів. Новачки дізнаються, на що здатні фішингові інструменти, здійснять свою першу аферу і бажають більшого, і саме тоді їм буде запропоновано платний контент. Інша причина розміщення подібних матеріалів – набір неоплачуваної робочої сили. Щоб залучити ширшу аудиторію, шахраї рекламують свої послуги, обіцяючи навчити інших фішингу за серйозні гроші. Таким чином основною небезпекою є навіть не самі атаки, а розповсюдження вказівок і ресурсів, завдяки яким кількість злочинців тільки зростає.

Враховуючі, що більшість кіберзлочинців не є професіоналами, їх методи можна назвати лінійними й обійти небезпеку стає простою задачею, коли знаєш на що звертати увагу. Одна з найпоширеніших хитрощів, які використовують шахраї під час фішингових атак – створення фейкової офіційної сторінки відомого бренду. Зловмисники схильні копіювати елементи дизайну з реального сайту, тому користувачам складно відрізнити підроблені сторінки від офіційних. Навіть доменне ім'я фішингової сторінки часто може виглядати як реальна веб-адреса певного бренду, оскільки кіберзлочинці додають до URL-адреси назву компанії або послуги, під якою вони видають себе. Цей трюк відомий як комбосквотинг. Злочинці, як правило, використовують зламані офіційні веб-сайти для розміщення сторінок, створених за допомогою фішингових наборів, або покладаються на компанії, що пропонують безкоштовний веб-хостинг. Останні постійно працюють над боротьбою з фішингом і блокують фейкові сторінки, хоча фішингові сайти часто за короткий період своєї діяльності встигають виконати поставлене завдання – зібрати та надіслати злочинцям персональні дані жертв. Посилання на таку сторінку звичайний користувач може отримати через розсилку бота, або групи. Як приклад, боти «Telegram» використовують обробку природної мови і штучний інтелект для ведення реалістичної розмови, що ускладнює визначення того, що вас обманюють. В одній із нещодавніх версій шахрайства хакери використовували бота, відомого як «SMSRanger», видаючи себе за

представників банків і компаній, таких як «PayPal», «Apple Pay», «Google Pay» і широко використовуваних операторів мобільного зв'язку. Щойно хакери вводять номер телефону користувача Telegram, бот дзвонить і переконує користувача надати особисту інформацію, логіни банківських рахунків, паролі і навіть коди двофакторної аутентифікації. Небезпека такого роду демонструє типові попереджувальні ознаки фішингового шахрайства, зокрема можна виділити наступні сім:

Використовує владу для завоювання довіри. Інтернет-шахраї використовують організації та імена, яким ви довіряєте, щоб послабити вашу пильність. Остерігайтеся тих, хто несподівано пише вам і стверджує, що він з IRS, уряду або відомої компанії.

Створює відчуття терміновості. Кіберзлочинцям потрібно, щоб ви діяли швидко, перш ніж ви зрозумієте, що вони задумали. Вони часто винаходять відчуття терміновості, щоб завадити вам спочатку перевірити їхні твердження.

Зв'язується з вами несподівано. Один із найпростіших способів виявити шахрая – це якщо він першим зв'яжеться з вами. Якщо ви отримали будь-яке повідомлення, телефонний дзвінок або електронний лист від когось, кого ви не знаєте, переконайтеся, що він той, за кого говорить, безпосередньо зв'язавшись з його агентством або компанією.

Запитує конфіденційну інформацію. Шахраї видають себе за ваш банк і запитують ваш PIN-код або онлайн-паролі, щоб «захистити» обліковий запис. Але законні фінансові установи ніколи не зроблять цього [3].

Надмірні обіцянки щодо того, що вони можуть виконати. Якщо щось або хтось здається «занадто хорошим, щоб бути правдою», велика ймовірність, що вас намагаються обдурити.

Намагається бути представницьким. Кіберзлочинці прикидаються другом або членом сім'ї, щоб швидко завоювати вашу довіру. Але це не так. Не довіряйте повідомленню тільки тому, що воно прийшло від знайомого вам облікового запису.

Змушує використовувати незвичайні способи оплати. Більшість варіантів онлайн-платежів захищають від шахраїв. Якщо хтось змушує вас заплатити йому невідстежуваним або незворотнім способом, це може бути шахрайством. Сюди входять банківські перекази, подарункові картки та криптовалюта.

Список використаних джерел

1. «WhatsApp, Viber and Telegram which is Best for Instant Messaging?», International Journal of Electrical and Computer Engineering (IJECE), June 2016.

2. Сєвєрінов, О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка, 2017. – С. 65-68.

3. Арчакова А.І., Сєвєрінов О.В. Аналіз забезпечення конфіденційності інформації в сучасних мессенджерах. Комп’ютерні та інформаційні системи і технології (2019).