Капуста Роман Дмитрович, здобувач вищої освіти факультету інфокомунікацій
Харківський національний університет радіоелектроніки, Україна

Науковий керівник: Євдокименко Марина Олександрівна, д-р. техн. наук, професор, професор кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

ЗБІР ОСОБИСТИХ ДАНИХ ЧЕРЕЗ СОЦІАЛЬНІ МЕРЕЖІ

Важко собі уявити сучасний світ без соціальних мереж та месенджерів. Щодня відправляється безліч повідомлень та переглядається величезна кількість публікацій з різних джерел в інтернеті, проте не кожен користувач мережі Internet замислюється над тим, як саме використовують його персональні данні та наскільки вони захищені від сторонніх очей.

Для користування будь-якою соціальною мережею (Facebook, LinkedIn, Instagram тощо) або іншим інтернет-ресурсом завжди необхідно пройти коротку реєстрацію та надати певну особисту інформацію про власника майбутньої сторінки. Зазвичай це ім'я, рік народження, стать та інші персональні дані, які за запевненням розробника, допоможуть покращити роботу інтернет-ресурсу для цього користувача. Однак у більшості випадків окрім вказаної інформації, інтернет-ресурси (додатки та сайти) збирають і інші дані, що стосуються технічних показників пристроїв з яких проводилася авторизація у системі, а також координати місцезнаходження пристроїв. Окрім цього, переважна більшість користувачів розміщують свої фото на сторінки, щоб індивідуалізувати себе та підтвердити автентичність вказаних даних. Дозвіл на збір подібної інформації надає сам користувач під час погодження з політиками безпеки та конфіденційності, які необхідно прийняти під час реєстрації на інтернет-ресурсі.

Таким чином, пройшовши реєстрацію користувач добровільно надає певну низку конференційної інформації, яку компанія при надані послуг використовує на власний розсуд. Зазвичай ці дані використовують для сортування пропозицій та товарів, які найбільше підходять користувачеві, також цю інформацію можна використати для статистики користувачів, які зареєстровані у даній соціальній мережі та інше. Результат цієї обробки даних користувач бачить майже миттєво: рекомендуються відповідні публікації, які користуються найбільшою популярністю серед користувачів подібної вікової категорії та гендерної приналежності. Після чого, користувачі починають наповнювати та індивідуалізувати власний обліковий запис задля створення віртуального переліку однодумців з певної теми розкриваючи, власний потенціал при створені публікацій або постів.

З точки зору комунікації, кожна соціальна мережа – це дуже потужний інструмент для створення груп однодумців з певних питань та інтересів. Окрім сторінок людей існують сторінки тварин, організацій, груп, компаній тощо. Через ці облікові записи також можна проводити збір інформації за інтересами людини. Так, наприклад, студенти або викладачі, з великої вірогідністю будуть підписані на сторінки власних кафедр та університетів. Додатково існують також соціальні мережі, в яких персональні дані та вподобання користувачів використовуються для

отримання роботи та приваблювання роботодавців. Прикладом такої соціальної мережі є всесвітньо відома мережа LinkedIn.

Проте, з точки зору безпеки, кожна соціальна мережа – це перше джерело отримання інформації для потенційного зловмисника. Збір даних про жертву у більшості випадків починається саме з відкритих джерел, якими являються соціальні мережі. Зловмисник, за допомогою, наприклад, технології OSINT (Open Source Intelligence), може отримати майже повну картину про свою ціль та використати прийоми соціальної інженерії для отримання власної вигоди.

Приклад збору даних з соціальних мереж

Для прикладу, проаналізуємо облікові записи однієї людини у двох всесвітньо відомих соціальних межах LinkedIn та Instagram. Ґрунтуючись на отриманих даних, можна побудувати профайл користувача та напрямок вподобань, які може використати зловмисник під час проведення атаки. З міркувань безпеки усі посилання на облікові записи та особисті фотографії людини будуть відкориговані. Для побудови профайлу користувача за допомогою мереж LinkedIn та Instagram потрібно виконати наступні кроки:

1. Аналіз сторінки Instagram.

Головна мета цього аналізу – визначення основного напрямку вподобань людини. Для цього потрібно провести огляд публікації та коментарів, що були залишені на сторінці користувача. Перша публікація приведена на рис.1.

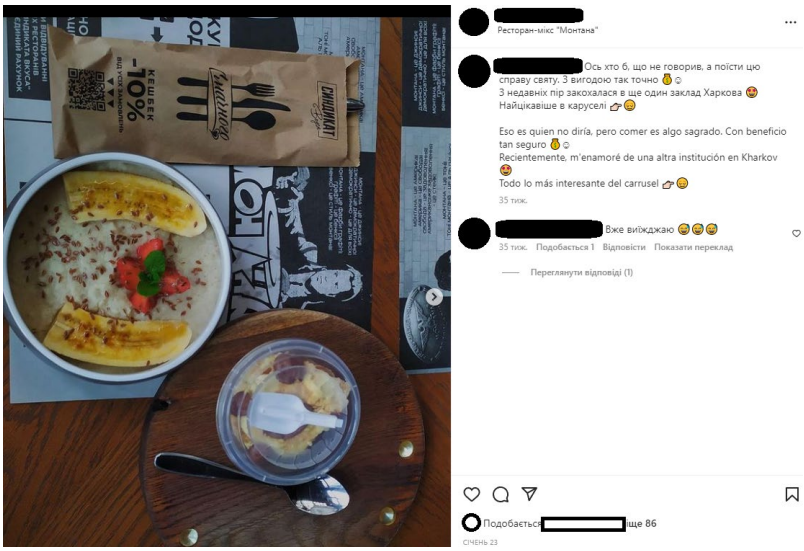

Рис. 1. **Огляд публікації сторінки Instagram користувача**

Після огляду публікації можна виділити певні важливі моменти, зазначивши те, що стає відомим справжнє ім’я користувача, дата народження та особисте фото. Вся ця інформація була надана у шапці профілю. Перше, що необхідно визначити, це вказану геолокацію закладу, вказаного в пості, та коментар автора стосовно нього. Після визначення геолокації стає зрозуміло, що заклад з посту користувача знаходиться в м. Харків. Ґрунтуючись на регулярності постів автору з цього закладу, можна зробити висновки, що ця людина проживає або буває у Харкові та може відвідувати цей заклад, тому що окрім публікації у січні місяці є згадування й у інші дати. Також слід зазначити те, що коментар до публікації написаний двома мовами українською та іспанською. Можливо автор подорожує до країн, де

використовується іспанська мова або вивчає її для загального розвитку. Слід зазначити, що дана публікація та усі інші, які розташовані на сторінці вказують на те, що це особистий блог користувача, бо переважна більшість подій висвітлюється у соціальних мережах, а значить можливо відслідкувати найчастіші переміщення та найулюбленіші заклади цієї людини.

2. Аналіз сторінки LinkedIn.

Продовжити аналіз обраного користувача можна зі сторінки LinkedIn та перегляду його облікового запису. Головна сторінка та основна інформація про користувача приведені на рис.2.

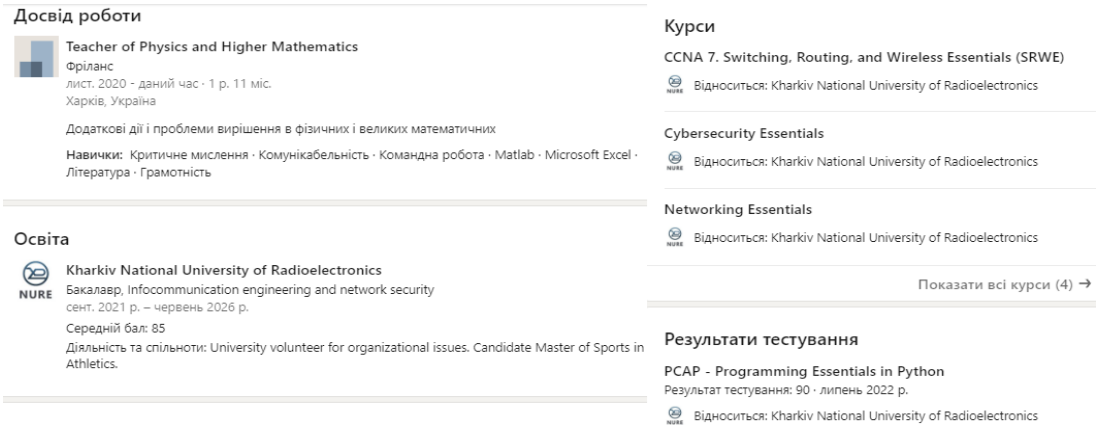

Рис. 2. **Огляд сторінки LinkedIn користувача**

Тут можна побачити, що обліковий запис містить велику кількість інформації про професійний розвиток користувача та вподобання. Перш за все можна визначити те, що людина навчається у Харківському національному університеті радіоелектроніки та має певну низку сертифікатів з профільних курсів. Додатково можна визначити, що власник сторінки постійно оновлює свій перелік пройдених курсів та отримує найрізноманітніші відзнаки, що свідчить про їх успішне закінчення.

Проаналізувавши отримані данні, потенційний зловмисник вже може побудувати певний вектор атаки на власника цих сторінок в залежності від цілі. Найпростіший та напевне найефективнішим методом атаки для цього випадку можна використати звичайний фішинг через особисте листування або через фейкові облікові записи. Зловмисник може приставитись, як менеджер якогось популярного харківського закладу та запропонувати купон на знижку під час наступного відвідування, а також приєднати до листа сам файл, начебто купона, проте він буде містити у собі шкідливий програмний код, який буде активовано при завантажені та відриті файлу. Подібним методом можна провести атаку через електронну пошту змінивши при цьому адресу таким чином, щоб вона майже не відрізнялась від оригіналу. Наприклад оригінальну адресу «noreply@stepik.org» змінити на «n0reply@stepik.org» або на щось подібне та сформувати лист запрошення на профільній курс, який відповідає вподобанню користувача та заманити таким чином до пастки.

Окрім зазначених методів зловмисник може використати дуже велику кількість варіантів атак спираючись на досить широкий спектр отриманих персональних даних з відкритих джерел, проте у будь-якому випадку слід

дотримуватися низки загальних правил, які допоможуть мінімізувати шкоду від переважної кількості атак із застосуванням соціальної інженерії.

1. Бути пильним та уважним. Не переходити за незнайомими посиланнями та не відкривати стороні листи. Уважно перевіряти електроні адреси.

2. Намагатися не розповсюджувати свої персональні дані та користуватися лише надійними інформаційними ресурсами.

3. Намагатися утримуватися від коментарів у соціальних мережах особливо під публікаціями, які мають провокуючий характер.

4. Користуватися функцією «Закритий профіль», для зменшення кількості переглядів особистих сторінок. З прискіпливістю відноситись до незнайомих контактів

Як висновок, слід зазначити, що безпека нашої інформації залежить тільки від нас та нашого оточення. Як казав Лорд Варіс: «Інформація - ключ до всього. Ви повинні дізнатися сильні сторони ваших ворогів і зрозуміти, хто з друзів вам зовсім не друг.»

Список використаних джерел:

1. Персональні дані онлайн: проблеми регулювання та перспективи захисту [Електронний ресурс] – Режим доступу до ресурсу: https://rpr.org.ua/news/personal-ni-dani-onlayn-problemy-rehuliuvannia-ta-perspektyvy-zakhystu/.