# МЕТОДИКИ РОЗСЛІДУВАННЯ ФІШИНГОВИХ АТАК З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ OSINT

Пічієнко М. Г.

Кафедра «Інфокомунікаційної інженерії
ім. В.В. Поповського», ХНУРЕ, Україна
E-mail: mariia.pichiienko@nure.ua

**Abstract**

*Phishing is the main attack vector for the majority of cyber-attacks. It also remains the most popular tool among both nation-state hackers and scammers, for different reasons. Apart from preventive measures cyber-security specialists can perform phishing attack investigation to report attribution to law enforcement or conduct threat analysis to improve internal cybersecurity policies.*

Фішинг є однією з найстаріших і найпоширеніших кіберзагроз. Кожен користувач Інтернету, від індивідуальних онлайн-покупців до менеджерів корпорації, може потенційно зазнати фішингових атак.

За різними даними з фішинга починаються від 60 до 90% усіх кібератак. Він також залишається найпопулярнішим інструментом як серед хакерів, так і шахраїв. Фішингова атака може містити веб-сайти, облікові записи або розсилки зі шкідливими архівами чи посиланнями. За даними компанії RangeForce за 2020 рік, 30% від усіх користувачів перейдуть по фішинговому посиланню, і 10% введуть дані своєї кредитної картки, не перевіряючи справжність сайту.

Але які дії необхідно вжити при виявленні фішингової атаки? Окрім простого уникнення натискання підозрілих URL-адрес або вкладень, спеціаліст з інформаційної безпеки може провести розслідування, щоб підтвердити спробу фішингу та оцінити рівень загрози. Таким чином, проведення фішингово розслідування необхідно, щоб:

- повідомити про спробу правоохоронним органам;
- провести аналіз загроз;
- удосконалювати внутрішню політику кібербезпеки та проводити тренінги з підвищення обізнаності.

Отже, розслідування фішингової атаки складається з наступних кроків.

Крок 1. Аналіз вихідних даних, пошук артефактів.

Починати розслідування слід з аналізу типу фішингової атаки (на які дані користувача направлена, є масовою розсилкою чи whaling атакою, тощо), часової шкали, методу розповсюдження, шкідливого змісту та основних показників (електронна пошта, ім’я вкладення, посилання, домени тощо).

Потім необхідно переглянути приманку, яка обманом змусила жертву відкрити шкідливий електронний лист або веб-сайт. Як правило, приманкою є електронна пошта, шкідливий код або фішинговий веб-сайт. Шукати можна такі артефакти, як:

- додатки, такі як підроблені платіжні документи;
- фішингові посилання, які часто маскуються під законні URL-адреси;
- відправлені/отримані часові позначки, які допомагають побудувати часову шкалу інцидентів, а іноді й визначити часовий пояс відправника;

- заголовки електронних листів (Envelope-From, Return-Path, Reply-to, Receive-From), які можуть дозволити вам отримати справжню адресу електронної пошти та домен зловмисника, навіть із підроблених даних електронної пошти;
- додаткові заголовки (X-PHP-SCRIPT, X-ORIGINATING-SCRIPT), які є рідкісними, але дуже цінними артефактами, які дозволяють дослідникам визначати конкретні сценарії пошти, URL-адреси, а іноді й IP-адресу.

Фішингові атаки можуть включати шкідливий код. Не обов'язково розбиратися, як само працює код, адже потрібні зачіпки найчастіше лежать на поверхні. Наприклад, IP-адреси та домени, що використовуються для зв'язку з командними серверами та серверами управління та зовнішніми ресурсами допоможуть під час аналізу інфраструктури зловмисника. Також у коді може міститися залишена контактна інформація розробників (наприклад, псевдоніми, адреси електронної пошти, контакти в месенджері).

В цільових розсилках часто зустрічаються URL-адреси, що ведуть на фішингові сайти. Аналіз фішингового веб-сайту включає:

- аналіз доступних реєстраційних даних WHOIS та записів DNS
- перевірку коду веб-сторінки
- перевірку форм та інтерфейсів авторизації
- відстеження мережевої активності, коли клієнтська програма взаємодіє з фішинговим веб-сервером.

Сервери, на яких розміщено фішинговий контент, заслуговують на особливу увагу. На цьому етапі проводиться сканування портів, пошук відкритих каталогів, проводиться фаззінг URL-адрес і виявлення вмісту, досліджуються сертифікати SSL та шукаються субдомени.

Основна мета аналізу вихідних об'єктів — знайти підказку, яка допоможе віднести фішингову кампанію. Вони варіюються від зовнішніх IP-адрес і нових доменів до рекламних ідентифікаторів, псевдонімів, номерів телефонів та електронної пошти. Звісно, кіберзлочинці не залишають свою справжню адресу чи номер телефону в коді фішингового сайту та не надсилають електронні листи зі своїх облікових записів (хоча і це іноді трапляється). Однак будь-яка дія залишає слід, і завдання аналітика — знайти якомога більше слідів і з'єднати точки.

Крок 2. Збагачення своїх знань про зловмисників.

Далі необхідно розширити свої знання про масштаби діяльності кіберзлочинців, виявляючи інші фішингові кампанії, нові й раніше невідомі інциденти, тестові проекти, ресурси, не пов'язані з хакерством, та їх найближче соціальне коло. Для цього можна використовувати інструменти OSINT, такі як:

- Maltego, Dirb, Dirhunt, DirBuster, Whois – розслідування сайтів, пошук каталогів;
- 2ip – перевірка IP-адреси;
- VerifyEmail, Email Reputation – перевірка email-адреси;
- Sherlock, Snoop, Namechk – пошук за нікнеймом;
- пошук у соціальних мережах за допомогою комплексних засобів, інструментів Google, внутрішніх інструментів для пошуку, тощо.

Зловмисники є людьми і схильні робити помилки, особливо на ранніх етапах своєї кримінальної кар'єри. Ось чому неправильна конфігурація сервера, помилково вказана особиста контактна інформація та нікнейми, можуть визначити юридичну сторону хакера.

Крок 3. З'єднання точок.

На даному етапі слід працювати з зібраною базою даних, що містить, наприклад, домени, псевдоніми, облікові записи на форумах хакерів і номери телефонів. Всі ці індикатори потрібно зливати в один довгий ланцюжок, що веде від оригінальної фішингової атаки до конкретної особи або групи.

Інструменти аналізу мережевих графів та системи аналізу загроз і атрибуції, які зберігають інформацію про інфраструктури супротивника (наприклад, IP, домени, сервери тощо), можуть бути надзвичайно корисними. Вони постійно оновлюють свої бази даних про суб'єктів загрози. Хоча повністю автоматизувати розслідування неможливо, використання цих інструментів суттєво зменшить обсяг роботи.

Довести причетність конкретних осіб до фішингової активності достатньо непросто. Спеціалісти з Group-IB стверджують, що для успішного ідентифікації особи необхідно привести хоча б три незалежні фактори, що вказують на зловмисника. Тому правильний підхід буде включати пошук якомога більшої кількості незалежної інформацію, яка б змогла допомогти підтвердити результат дослідження.

## *Література:*

1. 1. Kolmakov A. 5 Steps for Investigating Phishing Attacks [Електронний ресурс] – 11.03.2021. – Режим доступу до ресурса: https://www.darkreading.com/operations/5-steps-for-investigating-phishing-attacks

2. Phishing Attacks Part 1: What You Should Know About Phishing Activities [Електронний ресурс] – 20.10.2020. – Режим доступу до ресурса: https://www.maltego.com/blog/phishing-attacks-part-1-what-you-should-know/

3. Phishing Attacks Part 2: Investigating Phishing Domains [Електронний ресурс] – 09.11.2020. – Режим доступу до ресурса: https://www.maltego.com/blog/phishing-attacks-part-2-investigating-phishing-domains/