УДК 004.931

ОГЛЯД МЕТОДІВ ІДЕНТИФІКАЦІЇ КІБЕРАТАК НА ПРИКЛАДІ ІМПОСТОРІВ

А. В. Гаврилова[1], Г. О. Яйлимова[1]

[1] Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут

Анотація

У даній роботі розглядаються різні види загроз, котрі можна отримати через e-mail, особливу увагу приділено BEC (business e-mail compromise), виокремлено типи шкідливих електронних листів і їхні характерні риси.

Ключові слова: кібербезпека, кібератака, ідентифікація BEC, електронна пошта, електронні листи, спуфінг, інтернет-шахрайство

Вступ

Технічний прогрес подарував нам не лише корисні гаджети, розумні чати та можливість знайти будь-яку інформацію в інтернеті за лічені хвилини, але й появу нового типу тероризму – кібертероризму. Існує безліч його проявів: від булінгу в інтернеті до серйозних кібератак, котрі вражають системи по всьому світу (наприклад, вірус Petya, котрий був задіяний у масованій атаці в 2017 році). Що стосується пересічних громадян, вони мають ризик стати жертвами спроб зазіхання на приватні дані чи фінансові активи. У даній роботі буде розглянуто різні види загроз, що можуть бути отримані через електронне листування, їхні характерні риси; також більш детально поговоримо про BEC, розглянемо існуючі методи боротьби з цією загрозою, а також спробуємо сформувати способи ідентифікації імпосторів.

1. Види загроз

1.1. Загальні види загроз

Фішинг – шахрайські дії, що спрямовані на викрадення особистих даних отримувача (паролі, банківські рахунки, тощо). Дана загроза може бути реалізована за допомогою підроблених посилань або файлів, що копіюють зовнішній вигляд оригінальної сторінки з авторизацією для певного акаунту, або фейкових сторінок із оплатою товарів для інтернет-магазинів або інших рахунків, куди необачний отримувач може ввести свої банківські дані та стати жертвою зловмисників.

Скам – зловмисник намагається спровокувати отримувача на відповідь із метою подальшого шахрайства. Яскравим прикладом є «нігерійський скам» – випадок, коли в електронному листі до людини звертається ніби-то африканський принц і обіцяє великі гроші. Також до скаму належать повідомлення про виграш в лотереї, неочікувані величезні спадки, листи від багатих вдів, тощо.

Спам – вид шкідливих листів, до котрих належать небажані розсилки, реклама різних чудодійних медичних засобів, пристроїв, казино, а також контент 18+.

Малвар – шкідливе ПЗ, котре призначене для нанесення шкоди системі або «шпіонажу», що може бути отримане через вкладений файл у електронному листі або автозавантаження файлу за посиланням.

BEC (business e-mail compromise) або імпостор – вид шахрайства, котрий полягає в тому, що зловмисник видає себе за іншу людину (як правило – співробітника компанії) з метою отримання її привілеїв.

1.2. Види BEC

Імітація користувача – зловмисник на сторонньому домені створює пошту, що схожа на пошту користувача. Наприклад, замість пошти Івана Мартинюка на домені lll.kpi.ua буде пошта зловмисника на домені gmail.com: ivamar-ipt24@lll.com.ua –> ivamar-ipt24@gmail.com

Імітація адреси домену – зловмисник підробляє домен електронної пошти так, щоб він був схожий на оригінальний домен організації: lll.kpi.ua -> l1l.kpi.ua (друга літера «l» змінена на одиницю)

Спуфінг домену – зловмисник підробляє домен так, щоб він мав точно такий вигля як і домен організації. Оскільки вони абсолютно однакові, атака є більш переконливою. Протоколи електронної пошти спираються на стандарти автентифікації електронної пошти (SPF, DKIM і DMARC), щоб дозволити власникам доменів «автентифікувати» свою пошту. Якщо в домені не налаштовано ці параметри, шахрай має змогу підробити їх, щоб зробити електронний лист легітимним, але натомість він надходитиме з сервера електронної пошти зловмисника. Отримувач

бачить домен організації, але фактичний відправник інший.

Захоплення пошти – зловмисник дійсно має доступ до скриньки жертви, у такому разі отримувачу надсилаються електронні листи з реальної пошти відправника.

2. Існуючі методи ідентифікації BEC

Існують різні методи виявлення та запобігання BEC-атакам, які базуються на аналізі електронної пошти та її автентифікації.

2.1. Абсорбційна спектроскопія

Абсорбційна спектроскопія – перевірка стандартів автентифікації електронної пошти, таких як SPF, DKIM та DMARC, виявлення підроблених доменних імен. [1] В основі цього методу лежить принцип поглинання електромагнітного випромінення речовиною при певних довжинах хвиль. У контексті загроз, отриманих через e-mail, речовиною є електронна пошта, а довжинами хвиль – спеціальні записи DNS, що містять інформацію про дозволені джерела для кожного домену. Ці записи називають SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting and Conformance). Із їхньою допомогою отримувачі листів можуть перевіряти справжність електронної пошти, використовуючи криптографічні підписи та політики безпеки.

- **SPF** – це метод, котрий дозволяє визначити, які IP-адреси дозволені для відправлення електронної пошти від певного домену. SPF записується у вигляді DNS TXT запису на домені відправника та містить список IP-адрес або інших доменів, які можуть надсилати електронну пошту від цього домену. Отримувач електронного листа може перевірити SPF запис, щоб побачити, чи збігається IP-адреса відправника з дозволеними IP-адресами. [2]
- **DKIM** – це метод, що дозволяє підписувати електронні листи криптографічним підписом, який додається до заголовка e-mail-у. DKIM використовує пару ключів: приватний ключ, який зберігається на сервері відправника та використовується для підписання, і публічний ключ, який записується у вигляді DNS TXT запису на домені відправника та використовується для перевірки підпису. Отримувач електронної пошти може перевірити DKIM підпис, щоб побачити, чи не робилися зміни в листі після підписання. [3]
- **DMARC (Domain-based Message Authentication, Reporting and Conformance)** – це метод, що дозволяє задавати політику для того, як отримувач електронних листів повинен обробляти електронну пошту, яка не проходить SPF або DKIM перевірку. DMARC записується у вигляді DNS TXT запису на домені відправника та містить параметри, такі як:
  - p – політика для неавтентифікованих повідомлень, яка може бути none (не робити нічого), quarantine (перемістити до спаму) або reject (відхилити).
  - rua – адреса електронної пошти для отримання звітів про результати DMARC перевірки в агрегованому форматі.
  - ruf – адреса електронної пошти для отримання звітів про результати DMARC перевірки в індивідуальному форматі.
  - pct – відсоток повідомлень, до яких застосовується політика DMARC.
  - sp – політика для неавтентифікованих повідомлень із піддоменами, якщо вона відрізняється від основної політики.

  Приклад: "*v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@example.com; ruf=mailto:dmarc-failures@example.com; pct=100; sp=reject*" Це означає, що всі повідомлення з домену «example.com», які не проходять SPF або DKIM перевірку, повинні бути переміщені до спаму, а всі повідомлення з піддоменами "example.com" – відхилені. Звіти про результати перевірки надсилаються на дві різні адреси електронної пошти.

Якщо електронна пошта не має цих записів або не проходить перевірку, це може свідчити про те, що вона була вкрадена, або перехоплена зловмисниками, які намагаються обвести навколо пальця отримувача.

2.2. Виявлення червоних прапорців

Червоні прапорці, які можуть свідчити про підозрілу електронну пошту:

- несподіване або незвичайне прохання про переказ грошей, зміну банківських реквізитів або покупку подарункових карток,
- поганий синтаксис, граматика або орфографія в електронному листі [4],
- несподівана зміна країни отримання або імені бенефіціара,
- підроблена адреса електронної пошти (схожа на оригінальну, але з невеликими відмінностями, наприклад «facebook.com» –> «face.book.com»),
- обмеження варіантів відповіді на лист, наприклад: «Я у відпустці, тому ніяких дзвінків, тільки відповідь на цей лист»,
- невідповідність стилю або тону листа до типового способу спілкування відправника.

2.3. Рішення для захисту від фішингу

Застосування рішень для захисту від фішингу – використання спеціального ПЗ або сервісів, які можуть допомогти користувачам ідентифікувати та блокувати потенційно шкідливий вміст. Такі додатки можуть блокувати, перенаправляти або позначати

підозрілу електронну пошту та попереджати користувачів і адміністраторів про можливий ризик. [5] Приклади:

- Фільтрація вхідної та вихідної електронної пошти за допомогою безпечних електронних шлюзів (SEG), які перевіряють листи на наявність шкідливих посилань, вкладень, підроблених адрес і інших ознак фішингу.
- Використання хмарних технологій захисту, які сканують вхідну та вихідну електронну пошту на наявність складних загроз, таких як BEC, імітація VIP-осіб або захоплення облікових записів (ATO).

2.4. Навчання та освіта співробітників

Навчання та освіта співробітників – проведення тренінгів, семінарів і курсів цифрової грамотності, аби навчити співробітників розрізняти фішингові листи, перевіряти електронні листи на достовірність, не надавати конфіденційну інформацію чи грошові перекази без попереднього підтвердження, використовувати багатофакторну автентифікацію та повідомляти мережевого адміністратора про підозрілу активність. [6]. Найбільш поширений спосіб – SAT-інтеграції. Він полягає в тому, що здійснюється фішинг-тренінг кампанія (співробітникам розсилаються фішингові листи, але шкідливі посилання ведуть не на реальну загрозу від шахраїв, а на сторінку вендора, де написано, що користувач наткнувся на шкідливе посилання та даються рекомендації, як можна було б уникнути цієї ситуації.

Висновки

Результатами даної роботи є формування уявлення про різні види шкідливих електронних листів, їхні характерні риси, що допоможе не просто ідентифікувати потенційні загрози, а й запобігати інтернет-шахрайству; детально розглянуті імпостори та існуючі методи їхнього визначення. Практична цінність даної наукової роботи полягає в протидії кібертероризму, котрий є невід'ємною частиною гібридної війни, що охопила нашу країну.

Перелік використаних джерел

1. *Microsoft-Security.* What is Business Email Compromise (BEC)? — URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec.
2. *Gmail-Help.* Prevent mail to Gmail users from being blocked or sent to spam. — URL: https://support.google.com/mail/answer/81126?hl=en.
3. *Blackie A.* Email Authenticity 101: DKIM, DMARC, and SPF. — URL: https://support.google.com/mail/answer/81126?hl=en.
4. *microsoft.com.* Business Email Compromise Part One. — URL: https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900.
5. *Security-News.* Red Flags: How to Spot a Business Email Compromise Scam. — URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-to-spot-business-email-scam.
6. *FBI.* Business Email Compromise. — URL: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise.