BEC-АТАКА ТА OSINT: ІНСТРУМЕНТ ДЛЯ ПІДГОТОВКИ ДО ПРОВЕДЕННЯ АТАКИ ТА ІНСТРУМЕНТ ЗАПОБІГАННЯ У ОРГАНІЗАЦІЇ

Мицик М.В.

Кафедра «Інфокомунікаційної інженерії
ім. В.В. Поповського», ХНУРЕ, Україна.

E-mail: mariia.mytsyk@nure.ua

Abstract

Recently, there has been a clear trend in cybercrime to reduce the number of mass attacks and increase the number of targeted attacks. As before, the main focus of attacks is e-mail, but in a targeted attack on corporate e-mail, its impact on the work of the organization is much higher. Business Email Compromise Attack — a cyberattack involving the theft, substitution or personification of corporate e-mail. OSINT in turn is a powerful tool with which you can get useful information for both implementation of BEC-attack and prevention of it.

В останній час в кіберзлочинності спостерігається чітка тенденція до зниження кількості масових атак та підвищення кількості цільових атак. Як і раніше, основним направленням атак є електронна пошта, але при цільовій атаці на корпоративні електронні пошти, її вплив на роботу організації значно вищий. За останній рік кількість цільових атак підвищилась втричі, а отже і значно підвищилися фінансові втрати організацій, які атакують хакери.

Business Email Compromise Attack – кібератака, що включає викрадення, підміну або уособлення корпоративної електронної пошти. Цього року кількість шахрайств BEC у всьому світі зросла на 60%. Понад 90% організацій повідомляють, що зазнали цілеспрямованих атак на електронну пошту, а 23% організацій зазнають фінансових втрат. Залежно від розміру компанії, середні збитки від успішної схеми електронної пошти можуть становити 1,6 мільйона доларів і більше. Атака починається зі збору інформації про компанію: відомості про керівників та бухгалтерів, які виконують платежі, адреси електронної пошти співробітників, дані про контрагентів. За допомогою фішингу чи шкідливих програм злочинці компрометують облікові записи електронної пошти керівника, фінансистів та бухгалтерів, вивчають листування з контрагентами. Їхнє завдання — з'ясувати, яким чином відбуваються фінансові транзакції, хто запитує переклад, хто його підтверджує та хто безпосередньо виконує. OSINT в свою чергу є потужним інструментом, за допомогою якого можна отримати корисну інформацію як для проведення BEC-атаки так і для її запобігання.

Першим етапом проведення BEC-атаки є збір інформації про компанію. Злочинці використовують велику кількість інструментів OSINT для цього. Наприклад, для того, щоб знайти імена своїх цілей найефективнішим інструментом вважається соціальна мережа LinkedIn, яка збирає в собі аккаунти компаній та їх працівників, деякі контактні дані. Для знаходження електронних пошт працівників існує велика кількість онлайн-сервісів таких як: RocketReach, Snov.io, Hunter.io, Clearbit та інші. Вказані інструменти призначені для використання відділами маркетингу та продаж, але хакери також використовують їх для підготовки до атаки. Отримавши список існуючих адрес працівників компанії, злочинець аналізує формат назви електронної адреси для того, щоб створити підставну скриньку для проведення атаки, яка не викликає підозри у жертви атаки.

Повністю попередити збір відкритої інформації – неможливо, але можна зменшити кількість відкритих джерел, де злочинці можуть дізнатися електронні адреси працівників компанії. В першу чергу це розробка політики поводження з корпоративними поштовими

скриньками. Працівники не мають залишати свої корпоративні пошти на підозрілих сайтах, надавати логін та пароль до них, відкривати підозрілі листи.

Окрема політика має бути введена для керівників компанії та працівників фінансових відділів, адже вони є найчастішими жертвами BEC-атак. Їхні корпоративні пошти повинні мати двох-етапну верифікацію, не рекомендується залишати електронні пошти у відкритому доступі на веб-сайтах чи у соціальних мережах. Також необхідно проводити регулярний моніторинг джерел OSINT на наявність відкритих даних про поштові скриньки даних працівників. Корисним інструментом для цього є haveibeenpwned.com. Це безкоштовний онлайн сервіс, за допомогою якого можна перевірити факт витоку інформації за введеним електронним адресом. Скомпрометовані паролі відображатися не будуть, але хоча б можна буде розділити список адрес на "чисті" і потенційно скомпрометовані.

Так, як же використати OSINT для запобігання BEC-атаки у організації? Застосування наведених нижче найкращих практик допоможе краще захиститися від цих загроз і захистити системи ділової електронної пошти:

- створіть процес збору OSINT, який зосереджується на певних атрибутах, таких як зламані облікові записи електронної пошти співробітників або індикатори зловмисного програмного забезпечення;
- налаштуйте безпечну платформу для збору даних, яка відповідає внутрішнім бізнес-стандартам та стандартам безпеки даних;
- документуйте дані OSINT. Потім аналізуйте відносини за допомогою програми візуалізації даних або аналізу відносин;
- зберігайте загальнодоступні веб-сайти та соціальні мережі на наявність метаданих, які відповідають бажаним атрибутам OSINT;
- скануйте темну мережу на наявність даних, пов’язаних з вашим брендом або клієнтами;
- розробити процеси пом’якшення та відновлення для постраждалих бізнес-систем /клієнтів.

Висновки

Компрометація ділового листування відрізняється від звичайних атак мінімальною технологічністю. Успіх BEC-атак безпосередньо залежить від якості зібраної інформації та роботи соціальних інженерів.

Успішно виявляти та блокувати BEC-атаки дозволяє використання захисних систем на базі машинного навчання та штучного інтелекту у поєднанні з навчанням співробітників та іншими організаційними заходами.

Література:

1. How To Preven BEC Attacks [Електронний ресурс] / Socradar.io – Режим доступу до ресурсу: https://socradar.io/how-to-detect-bec-attacks/#3-How-to-Prevent-BEC-Attacks.
2. Як боротися з компромісом щодо ділової електронної пошти (BEC) за допомогою автентифікації електронної пошти? [Електронний ресурс] / Powerdmarc – Режим доступу до ресурсу: https://powerdmarc.com/ru/fight-bec-attack-with-email-authentication/.
3. Атаки на електронну пошту: тепер це особисте [Електронний ресурс] / Cisco – Режим доступу до ресурсу: https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/targeted_attacks.pdf.
4. Business Email Compromise: атака, від якої немає захисту [Електронний ресурс] / Trend Micro – Режим доступу до ресурсу: https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/targeted_attacks.pdf.