УДК 004.056:355.451

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРАТАК ТА КРАЩІ ПРАКТИКИ ДЛЯ ЗАХИСТУ ВІД НИХ

Качан В.Є., Нгуєн Х.Н.
Науковий керівник – к.т.н., доц. Куля Ю.Е.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, кафедра ІКІ імені В.В. Поповського, тел. +38(050) 702-55-92) email: vadym.kachan@nure.ua, khai.nhuien@nure.ua

This work is devoted to assessing current trends in attacks and best practices to protect against these attacks. The main trends that are not controlled by the security team are considered. Microsoft Security Intelligence Report and SANS (SysAdmin, Audit, Network and Security) Attack Threat Report are used. Common security controls have been identified as the best ways to improve protection.

Засоби масової інформації освітлюють багато порушень, збоїв та статистичних даних про кількість атак, здійснених у кіберпросторі. Однак треба ретельно шукати інформацію, щоб знайти надійні поради щодо виявлення та запобігання загрозам. Індустрія потребує експертного аналізу того, як менеджери з безпеки повинні розставляти пріоритети, щоб підвищити ефективність та результативність боротьби з відомими загрозами, а також мінімізувати ризики від нових атак.

Можна виділити три масштабних тенденції [1], кожна з яких не контролюється командою безпеки.

1. Винахідники постійно і не передбачувано придумують нові технології, протоколи та додатки. Зазвичай вони роблять це з акцентом на швидкість, простоту використання та прибутковість. На безпеку не робиться великий акцент.

2. Лідери бізнесу швидко впроваджують нові технології, а за ними і інші. Для інтеграції безпеки потрібен час, який компанії-першопрохідники не можуть собі дозволити, бо в такому випадку втратять свої переваги.

3. Хакери та злочинці швидко використовують вразливі місця.

Щорічний звіт Microsoft Digital Defense Report [2] є надійним джерелом тенденцій атак на комп’ютери та сервери Windows. У останній версії виявлено фішинг та BEC (Business Email Compromise, зловмисник за допомогою фішингу намагається обдурити компанію) як найпоширеніший початковий вектор атаки та виділила дві додаткові тенденції:

1. Зловмисники все частіше націлені на C-suite (найважливіша та найвпливовіша група осіб у компанії) та директорів, використовуючи

глибоке дослідження своїх цілей та використовуючи індивідуальні фішингові атаки.

2. Зловмисники у фішингових атаках все частіше видають себе за представників популярних брендів (торгових марок компаній) для підвищення випадків обману. Топ найпопулярніших брендів, за які себе видають зловмисники, а також топ 10 галузей для BEC-атак зображено на рисунку 1.

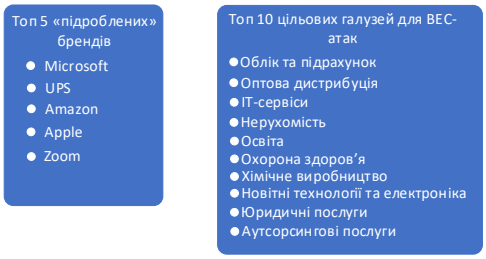

Рисунок 1 - Топ «підроблених» брендів та галузей для BEC-атак

Серед кращих методів покращення захисту виділяють загальні засоби контролю безпеки, які можуть зменшити ймовірність шкоди.

1. Уникнення багаторазових паролів. Фішингова атака, яка захоплює облікові дані та паролі привілейованих користувачів, уможливлює понад 70% усіх шкідливих атак. Дослідження Microsoft показали, що просте додавання SMS (Short Message Service) повідомлень як другого фактора аутентифікації зупинить 99,9% усіх фішингових атак. 2FA (2 Factor - двофакторна аутентифікація) не незламною, але вона піднімає планку проти зловмисників і змушує їх використовувати методи, які набагато легше виявити, ніж коли вони контролюють внутрішньо підключені ПК (Персональні комп'ютери).

2. Основна гігієна безпеки - керування конфігурацією, своєчасне виправлення, мінімізація привілеїв, сегментація мережі та контроль програм можуть запобігти ефективності більшості шкідливих виконуваних файлів, навіть якщо зловмиснику або програмі їх вдасться встановити.

3. Активний пошук загроз (threat hinting). Активний пошук аномалій і підозрілої поведінки для швидкого пошуку нових загроз зменшить збитки для бізнесу.

Список використаних джерел:

1. Pescatore J. SANS 2021 Top New Attacks and Threat Report [Електронний ресурс] / John Pescatore. – 2021. – Режим доступу до ресурсу: https://fs.hubspotusercontent00.net/hubfs/8645105/white-paper/sans-attack-threat-report-2021.pdf.

2. Microsoft Digital Defense Report [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.microsoft.com/en-us/security/business/security-intelligence-report.