УДК 004.056.5:004.75:004.8

Краєвський Ю.Р., здобувач,
Ящук В.І., к.екон.н., доцент,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

МЕТОДОЛОГІЯ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ФІШИНГОВИХ АТАК ІЗ ВИКОРИСТАННЯМ СИСТЕМИ ЗАХИСТУ ЕЛЕКТРОННОЇ ПОШТИ MICROSOFT DEFENDER FOR OFFICE 365

Фішингові атаки залишаються одним із найрезультативніших методів компрометації інформаційних систем, оскільки спрямовані на людський фактор і широко застосовуються для викрадення облікових даних, розповсюдження шкідливого ПЗ та здійснення фінансових шахрайств. У корпоративному середовищі ефективність протидії фішингу залежить від здатності системи безпеки аналізувати контент листів, перевіряти достовірність відправника, виявляти маніпулятивні або підозрілі елементи й блокувати шкідливу активність до взаємодії користувача з повідомленням. Microsoft Defender for Office 365 інтегрує набір механізмів, що базуються на машинному навчанні, сигнатурному аналізі та поведінкових алгоритмах, забезпечуючи багаторівневий захист поштової інфраструктури.

Фішингові кампанії ґрунтуються на підробці легітимної комунікації, модифікації заголовків та доменів, використанні шкідливих вкладень і гіперпосилань, що перенаправляють користувача на фальшиві ресурси. Виявлення таких листів потребує аналізу контексту повідомлення, автентичності доменів, структури тіла листа, конфігурації вкладень і параметрів мережевої взаємодії.

Система Microsoft Defender for Office 365 забезпечує багатовекторний захист електронної пошти завдяки поєднанню механізмів перевірки автентичності доменів, аналізу поведінки відправника та динамічної оцінки ризикових ознак листів у режимі реального часу. Microsoft Defender for Office 365 забезпечує глибоку перевірку вхідної кореспонденції шляхом застосування технологій anti-phishing policies, які оцінюють доменну репутацію, перевіряють SPF, DKIM і DMARC, аналізують ризикові шаблони поведінки відправника та виявляють підміну імені або адреси. Алгоритми машинного навчання моделюють сотні ознак електронного листа, включно з семантикою тексту, структурою HTML, характеристиками вкладень і метаданими, що дозволяє розпізнавати навіть складні таргетовані атаки.

Додаткову лінію захисту формує механізм Safe Links, який виконує динамічний аналіз URL-адрес у режимі реального часу та блокує доступ

до фішингових сайтів, навіть якщо початковий лист пройшов первинну перевірку. Функція Safe Attachments ізолює вкладення у віртуальному середовищі й досліджує їхню поведінку для виявлення ознак шкідливих скриптів, макросів або експлойтів.

Системи автоматизованого реагування (Automated Investigation and Response, AIR) виконують кореляцію інцидентів, ізолюють скомпрометовані листи у поштових скриньках, ініціюють блокування небезпечних відправників та виявляють взаємопов'язані загрози у масштабі всієї організації.

Поєднання технологічних механізмів із політиками доступу та навчанням користувачів формує цілісну систему протидії фішингу. Важливе значення має регулярне оновлення поштових політик, моделювання фішингових атак, контроль репутаційних атрибутів доменів та застосування багатофакторної автентифікації.

Методологія протидії фішинговим атакам у середовищі Microsoft Defender for Office 365 ґрунтується на багаторівневому аналізі електронних листів, поєднанні сигнатурних та поведінкових методів, використанні машинного навчання та ізоляції підозрілих елементів у спеціалізованих середовищах. Технології Safe Links та Safe Attachments дозволяють виявляти приховані форми фішингу та блокувати їх до того, як вони становитимуть ризик для користувача. Інтелектуальні механізми автоматизованого реагування забезпечують швидке усунення інцидентів і мінімізацію наслідків атак. Комплексність підходу створює основу для підвищення кіберстійкості організаційної поштової інфраструктури та зменшує ймовірність успішної компрометації користувачів.

Список використаних джерел:

1. Microsoft. Microsoft Defender for Office 365 Technical Documentation. Microsoft Docs, 2024. URL: https://learn.microsoft.com/microsoft-365/security/office-365-security/

2. National Institute of Standards and Technology. Trustworthy Email : NIST Special Publication 800-177. Gaithersburg : NIST, 2020. URL: https://csrc.nist.rip/publications/detail/sp/800-177/rev-1/draft

3. European Union Agency for Cybersecurity (ENISA). Phishing Threat Landscape 2023. Athens : ENISA, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

4. Mandiant Intelligence. Phishing Trends and Techniques Report 2024. Mandiant, 2024. URL: https://www.mandiant.com/resources