УДК 004

Макаревич С.О., здобувач
Дячук О.Ю., ст. викладач
Колощук М.С., ст. викладач
Державний університет «Житомирська політехніка»

HONEYPOT/HONEYNET У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ: СТРАТЕГІЯ ЗБОРУ ЕМПІРИЧНИХ ДАНИХ ДЛЯ ПРОГНОЗНОЇ БЕЗПЕКИ

У сучасних умовах зростання кількості кібератак та автоматизованих ботнет-кампаній корпоративні мережі перебувають у стані постійної загрози. Масові сканування, брутфорс-атаки та канали керування (Command and Control, C2) суттєво збільшують навантаження на служби безпеки. Традиційні методи, засновані на сигнатурах або статичних правилах, дедалі частіше демонструють недостатню ефективність у виявленні нових типів атак. Це зумовлює перехід від реактивної моделі захисту до прогнозної, що ґрунтується на аналізі поведінки зловмисників і закономірностей еволюції загроз.

У цьому контексті технології honeypot та honeynet виступають стратегічним елементом системи прогнозної безпеки. Вони дозволяють досліджувати реальну активність атакуючих агентів у контрольованому середовищі, формувати емпіричні бази даних і створювати моделі для передбачення загроз [1]. Їх наукова цінність полягає у можливості отримання автентичних даних про нові техніки атак та формування індикаторів компрометації (IoC), що збагачують системи виявлення (SIEM, SOAR).

Особливо актуальною є проблема нестачі якісних публічних датасетів із поведінкою ботнетів. Без них неможливе ефективне навчання алгоритмів ШІ та машинного навчання – основи адаптивних систем безпеки майбутнього [1]. Використання honeynet як контрольованого середовища здатне заповнити цю прогалину, забезпечуючи отримання реальних даних без ризику для продуктивних систем.

Концептуальна модель підходу передбачає гібридну архітектуру сенсорів. Сенсори низької взаємодії дають широку картину атакувальної активності, фіксують сканування та типові спроби вторгнення. Сенсори середнього й високого рівня взаємодії дозволяють досліджувати поведінку ботів, командні сесії, шкідливі файли та механізми C2-з'єднань [2], [3]. Отримані дані можуть бути використані для побудови поведінкових моделей виявлення загроз із застосуванням методів класифікації, машинного навчання та алгоритмів на кшталт

Random Forest, XGBoost чи LSTM, що підвищує точність прогнозної аналітики [3].

Наукова новизна підходу полягає у формалізації процесу створення репрезентативних honeynet-датасетів і методики оцінки переносності моделей між лабораторним та операційним середовищами. Важливим результатом є рекомендації щодо інтеграції даних із пасток у корпоративні системи моніторингу без істотного підвищення операційного ризику. Це створює основу для внутрішніх репозиторіїв загроз, що підсилюють аналітику в сучасних Security Operation Center (SOC).

Ключовим аспектом реалізації таких досліджень є дотримання етичних і правових вимог. Розгортання honeynet повинно супроводжуватися політикою data governance, що регламентує отримання дозволів, зберігання й анонімізацію даних та контроль вихідного трафіку для запобігання поширенню шкідливих артефактів. Практична імплементація має здійснюватися у співпраці з юридичними та кібербезпековими фахівцями, що гарантує технічну безпеку й відповідність міжнародним нормам.

Отримані результати важливі як для науки, так і для практики. Вони формують теоретичне підґрунтя розвитку поведінкової аналітики та підвищують ефективність систем моніторингу й реагування у корпоративних мережах. Honeynet як платформа прогнозного аналізу відкриває перспективи створення адаптивних систем кіберзахисту, здатних не лише реагувати на атаки, а й передбачати їх розвиток.

Дослідження підкреслює необхідність переходу до прогнозних моделей безпеки, де центральним елементом є збір та аналітика емпіричних даних. Використання honeypot/honeynet у корпоративних середовищах є науково обґрунтованим шляхом до формування нової парадигми кіберзахисту. Запропонована методологія дозволяє створювати безпечні експериментальні середовища для дослідження ботнет-активності, розвивати інструменти виявлення загроз і формувати основу для систем прогнозної безпеки наступного покоління.

Список використаних джерел:

1. Franco M., Abhishta A., Nieuwenhuis L., Joosten R. A Survey of Honeypots and Honeynets for Internet Security. arXiv:2308.10212, 2023. URL: https://arxiv.org/pdf/2108.02287

2. Fan W., Du Z., Smith-Creasey M., Fernández D. HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design // IEEE Journal on Selected Areas in Communications. 2019. Vol. 37, No. 3. P. 683–697. URL: https://arxiv.org/pdf/2402.06516

3. Yang X., Yuan J., Yang H., Kong Y., Zhang H., Zhao J. A Highly Interactive Honeypot-Based Approach to Network Threat Management // Future Internet. 2023. Vol. 15, No. 4. Article 127. URL: https://doi.org/10.3390/fi15040127