УДК 004.056

В.Р. Ружанський
О.В. Салієва

РОЗРОБКА MOVING TARGET DEFENCE (MTD) В АРХІТЕКТУРІ ZERO TRUST ARCHITECTURE (ZTA)

Вінницький національний технічний університет

Анотація

Робота присвячена розробці програмного засобу для активного захисту мережевих сесій на основі синергії архітектури нульової довіри (Zero Trust Architecture, ZTA) та технології захисту рухомої цілі (Moving Target Defense, MTD).

Ключові слова: Moving Target Defense, Zero Trust Architecture, Port Hopping, кібербезпека, активний захист, IoT.

Abstract

Work is dedicated to the development of a software tool for active network session protection based on the synergy of the Zero Trust Architecture (ZTA) and Moving Target Defense (MTD) technology.

Keywords: Moving Target Defense (MTD), Zero Trust Architecture (ZTA), Port Hopping, Cybersecurity, Active Defense, IoT (Internet of Things).

Вступ

Стрімкий розвиток інформаційно-комунікаційних технологій, глобальна цифровізація суспільства та перехід до хмарних інфраструктур супроводжуються експоненційним зростанням кількості та масштабу кібератак. Еволюція ландшафту кіберзагроз беззаперечно доводить, що традиційні методи захисту, орієнтовані виключно на створення міцного статичного периметра навколо корпоративної мережі (відомі як модель «замок і рів»), виявилися системно неефективними перед обличчям сучасних цілеспрямованих атак (Advanced Persistent Threats, APT), внутрішніх загроз та масового використання зловмисниками вразливостей нульового дня (Zero-Day).

Результати досліджень

Архітектура Zero Trust Architecture, (ZTA) та Moving Target Defense, (MTD) творить протидію мережевій розвідці шляхом перехоплення трафіку на неактивних портах та автоматичного блокування IP-адрес зловмисників на рівні ядра ОС. Динамічність зміни активних портів для прийому пакетів, а саме зміна через ΔT, надає обернено пропорційну ефективність системі.

Проведений експериментальний аналіз продемонстрував високу результативність запропонованої синергії.

За рахунок динамічного перестрибування портів ефективна поверхня атаки скорочується на 99.98% (з 16 383 до 3 доступних портів у кожен момент часу). Діаграма результативності активно/пасивних систем вказана на рис 1.

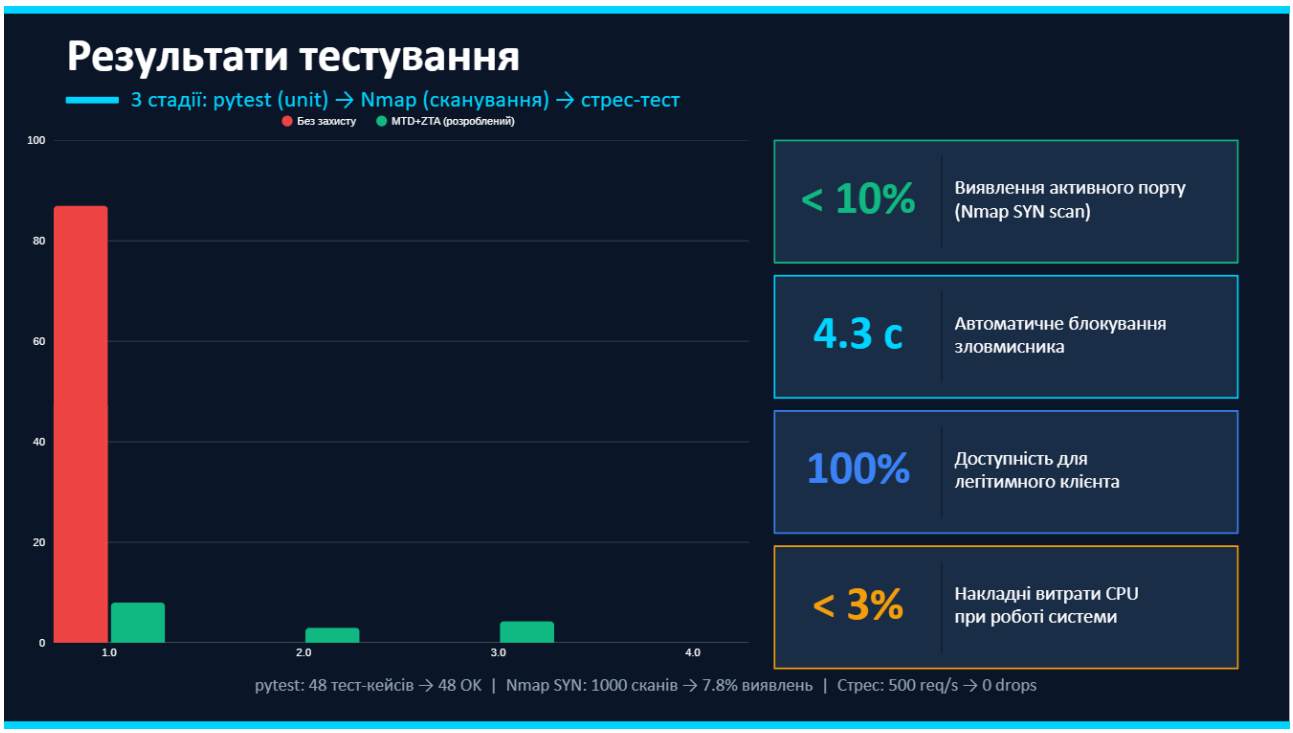

Рис. 1. Результати тестування виявлення активних портів в пасивно/активних системах захисту мережі

Рис. 1 показує, що активна система унеможливлює знаходження активного каналу передачі інформації в порівнянні до звичних пасивних систем у 10 разів.

Інтеграція з інструментарієм ядра ОС забезпечила автоматичне блокування IP-адрес зловмисників у разі спроб сканування або надсилання невалідних пакетів без переривання легітимних сесій.

Моделювання загрози за допомогою Cyber Kill Chain підтвердило, що MTD-захист руйнує етап розвідки (Reconnaissance) та унеможливлює підготовку експлойтів.

Висновки

Поєднання концепцій Zero Trust та Moving Target Defense є перспективним напрямком розвитку засобів кібербезпеки для IoT-систем та хмарних інфраструктур. Запропонований програмний засіб демонструє стійкість до активних мережевих загроз та забезпечує надійний захист даних навіть в умовах компрометації окремих сегментів мережі. Перспективи подальших досліджень полягають в оптимізації механізмів мутації за допомогою методів машинного навчання (DRL) для адаптивного вибору параметрів захисту залежно від поточного рівня загрози.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ковальчук Л. В., Савчук О. М. Забезпечення безпеки розподілених інформаційних систем. Інформаційні технології та комп’ютерна інженерія. 2023. № 2. С. 45–52.

2. Gerez-Soto M. et al. Going Beyond the Assumption of a Uniform Attack Model in Device Fingerprinting. IEEE Transactions on Dependable and Secure Computing. 2023. Vol. 20, No. 5. P. 3752–3767.

Ружанський Володимир Русланович – студент групи КІТС-22, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця

Салієва Ольга Володимирівна – д-р філософських наук, доцент, Вінницький національний технічний університет

Науковий керівник: ***Салієва Ольга Володимирівна*** – д-р філософських наук, доцент, Вінницький національний технічний університет, м. Вінниця

Volodymyr Ruslanovych Ruzhanskyi – Student, Group KITS-22, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia
Olha Volodymyrivna Salieva – Doctor of Philosophical Sciences, Associate Professor, Vinnytsia National Technical University

Academic Advisor: ***Olha Volodymyrivna Salieva*** – Doctor of Philosophical Sciences, Associate Professor, Vinnytsia National Technical University, Vinnytsia