УДК 004.75

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ БОТ-МЕРЕЖ

Цаволик Т. Г.[1)], Бондарчук М.Б.[2)]
Тернопільський національний економічний університет
[1)]к.т.н., викладач; [2)]магістрант

I. Постановка задачі

Бот-мережі стали однією з найбільших загроз для систем безпеки. Їх зростаюча популярність серед кіберзлочинців пов'язана з їх здатністю проникати майже до будь-якого пристрою, підключеного до Інтернету. Тому розробка нових методів і засобів, які б протидіяли бот-мережам і враховували перспективні можливості їх створення, функціонування та архітектуру засобів виявлення, є актуальною проблемою сьогодення.

II. Мета роботи

Метою роботи є аналіз відомих методів та алгоритмів для виявлення бот-мереж в середовищі.

III. Аналіз методів виявлення бот-мереж

Чимало науковців схиляються до методів виявлення бот-мереж за допомогою розподілених засобів, оскільки бот-мережі є керованим розподіленим програмним забезпеченням [1-2]. Зокрема, до них відносять мережні антивірусні засоби. При розробці методів та алгоритмів виявлення бот-мереж звертають увагу на: архітектуру бот-мережі (клієнт-серверна та децентралізована бот-мережі); аналіз трафіку із розробленими шаблонами даних про атаку; аналіз пакетів даних, що передаються і їхнє подальше порівняння із попередньо встановленими шаблонами атаки, що містяться в базі даних; дані про обмін інформацією між групами агентів із метою визначення рівня присутності бот-мереж; вміст зловмисного програмного забезпечення в локальних комп'ютерних мережах, що дає змогу здійснювати її наповнення різними функціоналами виявлення шкідливих компонентів.

Методи, що базуються на особливостях побудови та структури бот-мереж, представлена в роботах багатьох дослідників [3]. Такий підхід дозволяє змоделювати агентами архітектуру бот-мережі із різними механізмами їх функціонування. Основний недолік даного методу полягає в тому, що з кожним роком архітектури бот-мережі модифікують, поєднують та ускладнюють їхні структури, що ускладнює процес моделювання такої мережі для її подальшого дослідження. Базуючись на аналізі трафіку, зокрема, активні дослідження ведуться у напрямку DNS трафіку де дослідники виявляють бот-мережі, що дозволяє їм порівняти отримані результати аналізу трафіку з шаблонами бази аномалій [4]. Недоліком методів є необхідність постійного розбору трафіку та виділення важливих характеристичних ознак, які можуть змінюватись зловмисниками. При цьому не враховано архітектуру бот-мережі і блокування пакетів у подальшому не гарантує їх повторення. Один із методів виявлення бот-мереж ґрунтується на основі використання сигнатурного аналізу. Даний метод передбачає контроль кожного пакету, і його порівняння із попередньо налаштованими сигнатурами і шаблонами атаки, що містяться в базі даних. Недоліком методу є необхідність оновлення шаблонів, що впливає на ефективність виявлення нових бот-мереж.

Висновок

Відомі методи та засоби не забезпечують високого рівня достовірності у процесі виявлення нових бот-мереж. Це пояснюється застосуванням зловмисниками великої кількості різних технологій та методів приховування наявності та поширення бот-мереж у комп'ютерних системах, а також відставанням розроблених відомих методів.

Список використаних джерел

1. Rostami M.R. Botnet evolution: Network traffic indicators. / Eslahi M., Shanmugam B. and Ismail Z. - Biometrics and Security Technologies (ISBAST), 2014 International Symposium on, 2014. p.274−279.
2. Савенко В.О. Мережний метод виявлення файлового зловмисного програмного забезпечення в комп'ютерних системах локальних мереж. / В.О. Савенко. – вісник «Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки» Хмельницького національного університету, 2019 – С. 183-191
3. Kotenko I. Experiments With Simulation Of Botnets And Defense Agent Teams, ECMS 2013 - Proceedings edited by: W. Rekdalsbakken, R. T. Bye, H. Zhang, European Council for Modeling and Simulation.
4. Боровнікова К. Ю. Методи та програмне забезпечення інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка. 2016. автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 - інформаційні технології / Кіра Юліївна Бобровнікова. – Тернопіль : ТНТУ, 2017. – 23 с.