МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

АМБОК ВОЛОДИМИР ІВАНОВИЧ

УДК 004.056

АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІД DDOS-АТАК НА ОСНОВІ БОТНЕТІВ

125 "Кібербезпека”

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доктор технічних наук, доцент кафедри кібербезпеки **Александер Марек Богуслав**, Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: к.т.н., доцент кафедри інформатики та математичного моделювання Михайлишин М.С. **_____,** Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться 23 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії № ____ у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус № 1, ауд. 806.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Ботнет — це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів. За допомогою ботнетів часто надсилається спам, встановлюються шпигунські програми або здійснюється викрадення облікових даних користувачів. Масштабний ботнет може використовуватися для атак типу DDoS (Distributed Denial of Service) для спрямування додаткового трафіку на сайт та сповільнення роботи або збоїв підключення.

Шкідливі програми виду ботнет розповсюджуються за допомогою вкладень електронної пошти та через завантаження файлів і підроблених програм. Зловмисники також націлюються на такі уразливі місця, як неоновлене програмне забезпечення та відсутність захисту в мережі Інтернет. Все частіше під приціл зловмисників потрапляють камери, смарт-телевізори та навіть автомобілі.

Виявлення, а, відповідно, і захист від ботнетів є важливою і актуальною задачею. Обчислювальна потужність одного ботнету дозволяє здійснювати декілька зловмисних дій швидко та часто без виявлення. Наприклад, у 2016 році ботнет був використаний для створення найбільшої DDoS-атаки в історії, яка спричинила збої у роботі таких сайтів як Twitter, Amazon та Netflix.

Мета роботи: розгляд теоретичних та практичних засад технології виявлення інфікованих комп'ютерів, формалізацію створення методик виявлення.

Для досягнення вказаної мети в рамках дипломної роботи було сформульовано та розв’язано наступні задачі:

- розглянути принципи функціонування ботнетів для виявлення їх вразливих елементів з метою знешкодження;
- розглянути принципи виявлення ботнетів;
- виконати систематизацію інформації про протоколи обміну даними між ботнетами.

Об’єкт, методи та джерела дослідження: процес виявлення шкідливого програмного забезпечення.

Методи дослідження. Для досягнення мети дипломної роботи використовувались:

– методи узагальнення та аналізу – при проведенні огляду стану загроз на основі ботнетів;

– формалізації та математичного моделювання – при розробці методу виявлення вторгнень на основі статистичних методів.

Предмет дослідження: способи виявлення ботнетів на основі різноманітних підходів і принципів.

Наукова новизна отриманих результатів.

Наукова новизна полягає у вирішенні задачі систематизації відомостей про засоби виявлення та запобігання атак на хмарні мережеві сервіси зараженими обчислювальними вузлами. При цьому було отримано такі результати:

– на основі класифікації загроз від ботнетів запропоновано використовувати системи виявлення вторгнень на основі нейронних мереж;

– виокремлено переваги та недоліки систем виявлення вторгнень на основі різних принципів;

– вироблено рекомендації стосовно використання систем виявлення вторгнень.

Практичне значення отриманих результатів.

Всі розроблені методи можуть бути доведені до практичного впровадження у складі системи захисту від ботнентів. Така система дозволить мінімізувати ризики від шкідливої діяльності ботнетів.

Апробація. Основні положення роботи доповідались, розглядались та обговорювались на науковій конференції Тернопільського національного технічного університету. Результати дипломної роботи опубліковані у 1 науковій праці, яка є тезами студентської наукової конференції, яка проводились у ТНТУ.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – ____ арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі розкрито актуальність теми, окреслено основні завдання на дипломну роботу.

В першому розділі виконано аналітичний аналіз поставленого завдання та систематизовано матеріал, що стосується систем виявлення вторгнень на мережеві хмарні сервіси.

В другому розділі здійснено аналіз найбільш відомих ботнетів та досліджено принципи їх комунікації, поширення і способів шкідливого впливу на розподілену систему.

В розділі практичної реалізації описано методи та проект системи для визначення заражених мережевих вузлів на основі статистичних підходів. Запропоновано архітектуру такої системи та подано її псевдокод для подальшої програмної реалізації.

В спеціальній частині здійснено аналіз основних видів атак ботнетів та шкоду, котру вони можуть спричинити для різних видів бізнесової діяльності.

В частині «Обґрунтування економічної ефективності» розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень.

В частині «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання планування робіт по охороні праці та аналіз небезпек природного походження та антропогенного походження.

В частині «Екологія» проаналізовано сучасний екологічний стан України, розглянуто питання забруднення довкілля, що виникає внаслідок використання комп'ютерної техніки, а також запропоновано заходи зі зменшення цього негативного впливу.

У загальних висновках щодо дипломної роботи описано прийняті в проекті технічні рішення і організаційно-технічні заходи, які забезпечують виконання

завдання; оригінальні технічні рішення, прийняті автором в процесі роботи; технічні рішення роботи, які можуть бути впроваджені практично.

В додатках до пояснювальної записки приведено копії тез доповідей на студентській науковій конференції.

ВИСНОВКИ

У цьому дослідженні були вивчені існуючі моделі машинного навчання в контексті виявлення ботнетних мереж P2P. І була запропонована краща модель для штучних нейронних мереж на основі байєсівської регуляризації, яка є дуже ефективною в контексті проблеми, яка потребує хороших узагальнюючих здібностей.

Таким чином, за допомогою статистичних тестів остаточно показано, що навчена модель BR-ANN здатна дуже добре узагальнити і здатна передбачити активність невідомих шкідливих дій ботів. Виявлення конкретного виду шкідливої діяльності та тим самим ідентифікація невідомого бота може допомогти експертам з безпеки вжити відповідних профілактичних заходів.

Завдяки великій пропускній здатності мережі, перехід на масштабовану та розподілену архітектуру є дуже привабливою альтернативою. Інтеграція пропонованої системи API Hadoop API відповідно до парадигми Map-Reduce – можливий майбутній напрямок розвитку цієї роботи.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Яворський Р. Проблеми інформаційної безпеки при розгортанні системи виявлення вторгнень [Текст] / Р. Яворський, В. Амбок, В. Леньо. Матеріали науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2019. – с. 108.

АНОТАЦІЯ

Ботнет – це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів. За допомогою ботнетів часто надсилається спам, встановлюються шпигунські програми або здійснюється викрадення облікових даних користувачів. Масштабний ботнет може використовуватися для атак типу DDoS (Distributed Denial of Service) для спрямування додаткового трафіку на сайт та сповільнення роботи або збоїв підключення.

Шкідливі програми виду ботнет розповсюджуються за допомогою вкладень електронної пошти та через завантаження файлів і підроблених програм. Зловмисники також націлюються на такі уразливі місця, як неоновлене програмне забезпечення та відсутність захисту в мережі Інтернет. Все частіше під приціл зловмисників потрапляють камери, смарт-телевізори та навіть автомобілі.

Виявлення, а, відповідно, і захист від ботнетів є важливою і актуальною задачею. Обчислювальна потужність одного ботнету дозволяє здійснювати декілька зловмисних дій швидко та часто без виявлення.

Ключові слова: БОТНЕТ, ЗАГРОЗА, ІДЕНТИФІКАЦІЯ БОТНЕТІВ, ПРОТОКОЛ.

ANNOTATION

Botnet is a network of computers infected with malware. Cybercriminals use botnets that consist of a large number of computers for various malicious activities without the knowledge of users. Botnets often send spam, install spyware, or steal user credentials. A large-scale botnet can be used for DDoS (Distributed Denial of Service) attacks to direct additional traffic to the site and slow down work or connection failures.

Botnet-type malware is spread through email attachments and through file downloads and fake applications. Attackers also target vulnerabilities such as uninstalled software and a lack of Internet security. Increasingly, the target of intruders is cameras, smart TVs and even cars.

Detecting and, accordingly, protecting against botnets is an important and urgent task. The computing power of a single botnet allows several malicious actions to be performed quickly and often without detection.

Key words: BOTNET, THREAT, BOTNET IDENTIFICATION, PROTOCOL.