УДК 004.056

Н. Р. Кондратенко
О. М. Никитюк

ВИЯВЛЕННЯ АНОМАЛІЙ НА ОСНОВІ СТОХАСТИЧНОЇ НЕЙРОТЕХНОЛОГІЇ

Вінницький національний технічний університет

Анотація: *у даній роботі досліджено проблему мережевих атак на відмову в обслуговуванні. Розглянуті наявні методи захисту від DDoS-атак.*
Ключові слова: *DDoS-атаки, захист інформації, кіберзлочинці.*

Abstract: *Explored problem of network attacks on denial of service. Considered existing methods of protection form DDoS attacks.*
Keywords*: DDoS attacks, information security, cybercriminals.*

На сьогоднішній день атаки відмови в обслуговувані найбільш популярні, так як вони дозволяють привести до відмови майже будь-яку систему. Жертвами таких атак може бути будь-який ресурс відкритий ресурс. Повністю захиститись від DDoS-атак неможливо, так як не існує повністю надійних систем. Тому виникає проблема пошуку методів для захисту від атак відмови в обслуговуванні.

Число атак з відмови в обслуговуванні в другому кварталі 2015 року досягли рекордно високого рівня, відповідно до останніх доповіді від Akamai. Перше місце серед країн з яких проводилися DDoS-атаки займає Китай, після нього йдуть США і Великобританія.

DDoS-атаки стали звичайним засобом кіберзлочинців, щоб відволікти охорону цілі. У Великобританії було скоєно DDoS-атаку на компанію продажу мобільних телефонів Carphone Warehouse, і в цей же час хакерами було викрадено мільйони клієнтських даних[1]. За результатами дослідження, проведеного фахівцями Лабораторії Касперського і B2B International, DDoS-атаки на інтернет-ресурси компанії може привести до значних втрат - з середніми значеннями в діапазоні від $ 52000 до $ 444000 в залежності від розміру компанії. Для багатьох організацій ці втрати серйозно впливають на положення компанії серед конкурентів, а також наносять шкоду репутації через втрату доступу до інтернет-ресурсів для партнерів і клієнтів[2].

Для захисту використовують різні методи. DDoS-атаки розглядаються як проблема перевантаженості контролю, а тому більшість таких заторів викликано шкідливими хостами, які не підкоряються традиційному контролю перевантаження. Функціональність додається до кожного маршрутизатора для виявлення і відкидання пакетів, які, ймовірно, належать до атаки[3]. Хмарні провайдери надають захист від DDoS-атак. Вони надають досить велику пропускну здатність, що не дозволяє більшості DDoS-атак нанести будь-яку шкоду. Крім того хмарні ресурси зберігаються розподілено, і при відмові одного їх сховищ інші будуть доступними[4].

Метод для виявлення DDoS шляхом побудови нечіткої оцінки основаної на середньому часі прибуття пакетів. Проблема розділена на дві проблеми, перша з яких фактичне виявлення, для DDoS-подій, а другий ідентифікація IP-адрес порушника. Введені суворі обмеження в режимі реального часу для першого виклику і більш слабші обмеження для ідентифікації адрес. Через емпіричні оцінки підтверджено, що виявлення може бути завершене в межах реального часу і за допомогою нечітких оцінок замість чітких статистичних описів можливо уникнути недоліків, пов'язаних з припущеннями про моделі розподілу трафіку. Крім того, вдалося отримати результати у проміжку виявлення 3 сек[].

Виявлення та захист від DDOS-атак методами пакетної передачі даних включає в себе: блок збору інформації потоку для збору, з одного або більше вхідних пакетів з IP-адресою в цільовому нападі системи на IP-адресу призначення, потік інформації, у тому числі джерело IP-адреси вхідних пакетів і пакетів пунктам одним або декількома потоками, які класифікуються для кожної з IP-адреси джерела і кожного з різних типів протоколів; огляд блоку для розрахунку пакетів в секунду (PPS) значення потоків на основі графів пакетів; і блок відгуку для визначення способу реагування атаки

DDoS для кожного з потоків на основі значення PPS і типу протоколу відповідного потоку, що обробляє відповідний потік з використанням певної DDoS методу атаки[6].

Застосування нейронних мереж дозволило створити «інтелектуальну» систему, в якій детектори здатні ефективно виявляти не тільки відомі, але і невідомі комп'ютерні атаки[7]. Перевагою у використанні нейромережевого підходу при виявленні аномалій в мережевому трафіку є гнучкість, яку ці мережі надають[7]. Система на основі нейронної мережі ідентифікує ймовірність того, що окрема подія, або серія подій вказують на те, що проти системи здійснюється атака. Нейромережа здатна аналізувати неповні або перекручені дані, одержувані з мережевого трафіку Здатність обробляти дані від великої кількості джерел є особливо важливою при розгляд розподілених атак, проведених проти мережі скоординованими численними атакуючими. Найбільш важлива перевага нейромереж при виявленні аномалій мережевого трафіку полягає в її здатності до вивчення характеристик умисних атак та ідентифікації елементів, які не схожі на ті, що спостерігалися в трафіку колись. Таким чином, нейромережі володіють адаптивністю, що дуже важливо для забезпечення сучасної інформаційної безпеки[8].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. DDoS attacks hit record numbers in Q2 2015. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.digitaltrends.com/computing/ddos-attacks-hit-record-numbers-in-q2-2015 - назва з екрану.
2. A single DDoS attack can cost a company more than $400,000. [Електронний ресурс]. – Режим доступу до ресурсу : http://www.kaspersky.com/about/news/business/2015/A-single-DDoS-attack-can-cost-a-company-more-than-400000-dollar - назва з екрану.
3. Implementing Pushback: Router-Based Defense Against DDoS Attacks [Електронний ресурс]. – Режим доступу до ресурсу : http://academiccommons.columbia.edu/catalog/ac:126886 - назва з екрану.
4. VP of Technology, Verisign, special to Network World. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.networkworld.com/article/2170051/tech-primers/tech-primers-four-ways-to-defend-against-ddos-attacks.html – назва з екрану.
5. An intelligent method for real-time detection of DDoS attack based on fuzzy logic [Електронний ресурс]. – Режим доступу до ресурсу: https://www.researchgate.net/publication/225379905_An_intelligent_method_for_real-time_detection_of_DDoS_attack_based_on_fuzzy_logic- назва з екрану.
6. DDoS attack detection and defense apparatus and method using packet data [Електронний ресурс]. – Режим доступу: URL https://www.google.com.tr/patents/US8634717 - Назва з екрану
7. Виявлення мережевих аномалії на основі нейромережевих технологій. [Електронний ресурс]. – Режим доступу до ресурсу: http://ua.nauchebe.net/2015/04/viyavlennya-merezhevix-anomali%D1%97-na-osnovi-nejromerezhevomu-texnologij/- назва з екрану.
8. Кондратенко Н. Р., Куземко С. М. Основи нейромереж. Теорія і практика. Навчальний посібник, ВНТУ. – 2006.

Никитюк Олесь Миколайович, студент, Вінницький національний технічний університет, м. Вінниця, факультет інформаційних технологій та комп'ютерної інженерії, 1БС-12б, olesnk21@gmail.com

Кондратенко Наталя Романівна, к.т.н., професор кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Nykytiuk Oles Mykolayovuch, student, Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, 1BS-12b, olesnk21@gmail.com

Kondratenko Natalya Romanivna, Ph.D. professor of Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, chair of information security.