УДК 004.738

ШЛЯХИ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ВПЛИВУ DDOS-АТАК НА ІНОРМАЦІЙНІ РЕСУРСИ

Поковба О. Ю., Правило В. В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: pokovba.alexander@lll.kpi.ua, v.v.pravylo@ukr.net

WAYS TO DETECT AND NEUTRALISE THE IMPACT OF DDOS ATTACKS ON INFORMATION RESOURCES

The study examines normalization techniques to enhance detection accuracy. The results demonstrate that anomaly detection methods can effectively identify the onset of DDoS attacks and help mitigate malicious traffic.

Щоб ефективно виявляти різні DDoS-атаки, потрібно більше зосередитися на виявленні спільних властивостей цих зловмисних атак. Однією з таких властивостей є змінність вихідних IP-адрес, які генерують атакуючі пакети [1]. Ентропія мінливості пакетів H(Z) визначається за допомогою формули (1), яка визначається як сума Zi – об’єму пакетів, надісланих між парою з’єднань джерела та призначення (IP-адреси джерела та призначення, тобто src-dst IP) – і p(Zi) ймовірності його знаходження, вираженої шляхом нормалізації загальної кількості пакетів на Zi [2].

$$H(z) = -\sum_{i=1}^{n} zi \log(p(zi)) \quad (1)$$

Потім значення ентропії нормалізується з максимальною ентропією (2), де N - кількість різних пар зв'язку (src-dst IP).

$$H(N) = \log(N)/\log(2) \quad (2)$$

Значення ентропії вимірює, наскільки широко пакети розподіляються по розподілу. Здається, ентропія та різноманітність змінюються під час DDoS-атаки. Оскільки реальний трафік різноманітний, значення ентропії змінюються набагато різкіше, ніж будь-коли. Значення ентропії можуть змінюватися досить швидко, оскільки через характер різних служб [3], які вимагають різної швидкості передачі даних, структура потоків даних стає непостійною. Така зміна кожного другого випадку ускладнює визначення чіткого порогу виявлення DDoS-атаки. Щоб гарантувати, що він керує прийняттям обґрунтованих рішень, повинен існувати фільтр ентропійних даних, роль якого полягає у вилученні правильного набору значень [4]. Метод передбачає фільтрацію ентропійних даних із роздільною здатністю більших 10-секундних інтервалів із вибором максимумів, які можуть представляти їх для цього інтервалу (рис. 1).

$$F(z) = \max(zi, i = 1..10) \tag{3}$$

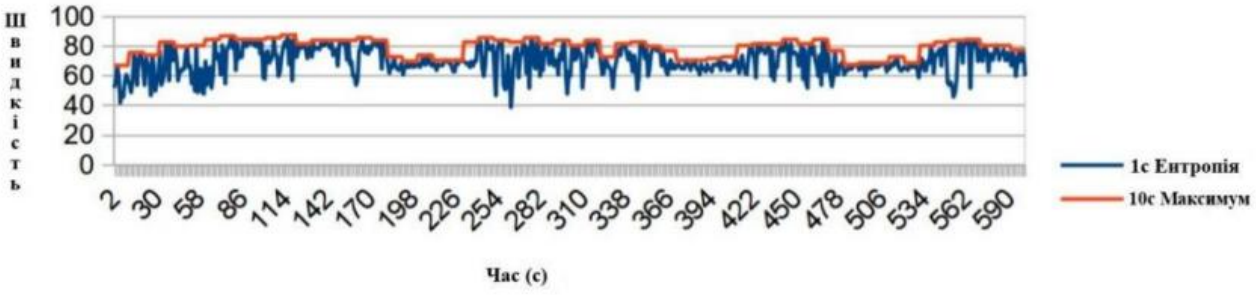

Рис.1. Найвищі значення швидкості у проміжках в 10с.

Суть запропонованої стратегії ідентифікації DDoS-атак та шкідливого трафіку полягає в інноваційному алгоритмі максимально оперативного визначення початкової точки розподіленої атаки, метою якої є знесення системи. Алгоритм також має можливість враховувати коливання сезонного навантаження, що гарантує значно більшу точність і швидкість розпізнавання атаки на її початковій стадії [5]. Крім того, було проведено ретельне дослідження, щоб підтвердити саме існування сезонних закономірностей і знайти типові сезонні періоди. Це дослідження показало, що деякі існують, тижнева і добова сезонність, і досить нечітко виражені, а також причини різкої добової сезонності.

Програмне рішення (рис. 2) застосовне для ефективного захисту «останньої милі», яка є найбільш критичним сегментом мережі. Основною функцією даного комплексу є забезпечення безпеки веб-серверів від DDoS-атак у вигляді http-флуду. Програмне забезпечення має широкий діапазон операційних систем, сумісне з усіма сучасними веб-серверами. Крім того, цей програмний комплекс можна встановлювати не тільки на фізичних серверах, а й використовувати у віртуальних хостингових середовищах, що дає можливість забезпечити масштабованість і гнучкість захисту.

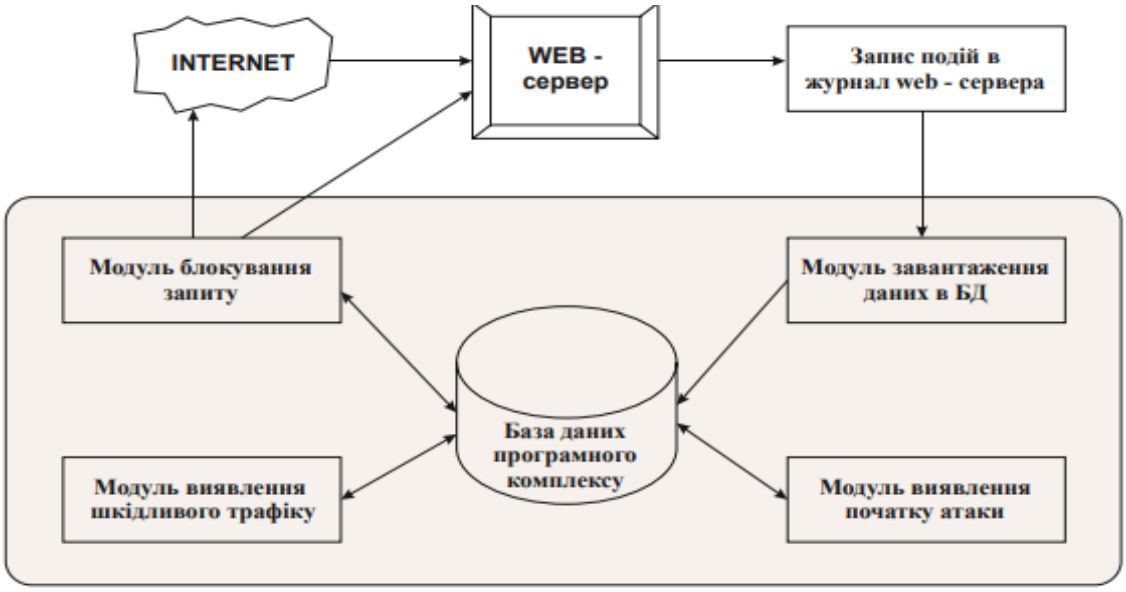

Рис.2. Архітектура програмного комплексу.

Універсальність програмного комплексу виявлення та протидії DDoS-атакам може бути реалізована не тільки для виявлення http-flood, але й для більшої кількості типів DDoS-атак. Трохи змінившись, програмне забезпечення може обробляти дані з лог-файлів різних мережевих служб, оскільки не є основним модулем, тому, крім мережевих локаторів, можна використовувати кілька інших фрагментів інформації. У цій реалізації весь програмний комплекс складається з трьох модулів і розміщується на кінцевому мережевому ресурсі. При необхідності програмні модулі можна розмістити будь-де в мережі. Так, наприклад, кінцевий сервер може мати лише завантажувач даних. Інструменти виявлення атак і фільтрації трафіку можна встановити на окремому сервері, який неможливо атакувати із зовнішньої мережі [6]. У такому встановленому програмному забезпеченні сервіс буде здатний нормально функціонувати та класифікувати трафік навіть у разі збою атакованого сервера.

Опція інсталяції доступна, якщо на захищеному вузлі не встановлено програмні модулі; звичайно, якщо дані можна отримати з мережевих локаторів та/або маршрутизаторів. В іншому випадку можна здійснити блокування трафіку на наступному вузлі [7]. Також програмний комплекс підтримує мультиінсталяцію при одночасному запуску декількох модулів виконуваного об'єкта з однаковою назвою. Наприклад, дані, на основі аналізу яких буде прийнято рішення, можуть надходити в базу з кількох джерел. На різних рівнях дані про зловмисний трафік можуть надсилатися в процесі блокування рекомендацій.

Література

1. Виявлення DDoS-атак (DDoS) Офіційний сайт компанії Cisco [Електронний ресурс]. Режим доступу : http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900
2. Карта DDoS-атак в реальному часі [Електронний ресурс]. - Режим доступу: URL : http://www.digitalattackmap.com/
3. Арун Радж Кумар, П. та С. Селвакумар, "Розподілена загроза відмови в обслуговуванні (DDoS) в середовищі спільної роботи - огляд інструментів DDoSатак та механізмів відстеження", Міжнародна конференція з перспективних обчислень (IACC 2009), сс. 1275-1280, березень 2009
4. Д. Діттріх, Г. Вівер, С. Діттріх, Н. Лонг, "Інструмент атаки на розподілену відмову в обслуговуванні Mstream", травень 2000.
5. Алекс Дойал, Джастін Чжан та Хуймінг Анна Ю, "На шляху до перемоги над DDoS-атаками", Міжнародна конференція з кібербезпеки, с. 209-211, 2012 IEEE.
6. Rocky K. C. Chang, "Захист від розподілених атак на відмову в обслуговуванні на основі переповнення: Підручник", IEEE Communications Magazine, стор. 42-51, жовтень 2002.
7. AT&T Center for Internet Research at ICSI Аналіз використання рефлекторів для розподілених атак на відмову в обслуговуванні,
[online] http://www.icir.org/vern/papers/reflectors.CCR.01.pdf.