ВИЯВЛЕННЯ DDOS-АТАК НА DNS-СЕРВЕР ЗА ЧАСОВИМ РЯДОМ УЗАГАЛЬНЕНОЇ ХАРАКТЕРИСТИКИ ТРАФІКУ

Зінченко В. В., магістрант; Зінченко М. В., к.т.н.
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

Сьогодні DDoS-атаки створюють суттєві загрози безпеці комп'ютерних систем. Прийоми атак передбачають використання різних підходів та засобів, які стають все потужнішими та можуть перенаситити будь-який «онлайн хост» або сервіс. Можливий катастрофічний наслідок від цих атак, пов'язаний зі враженням основних компонент інфраструктури Інтернету, таких як DNS-сервери.

DNS-сервер є сервісом, що встановлює відповідність між доменними іменами та IP-адресами, тобто фактично використовується в усіх інших службах і протоколах мережі. Як наслідок, вихід з ладу навіть незначної частини DNS-інфраструктури протягом невеликого проміжку часу може спричинити значний хвильовий ефект «замирання», що стрімко зростає.

DNS-протокол не підлягає шифруванню протягом процесу передачі. У якості транспортного протоколу використовується UDP-протокол, котрий, на відміну від TCP-протоколу, не виконує трьохстороннього зв'язку і взагалі не встановлює з'єднання з адресатом. За таких умов неважко підмінити IP-адресу джерела. На невеликі DNS-запити сервери можуть дати DNS-відповідь великого розміру. Таким чином, DNS-сервери є популярними об'єктами для DDoS-атак [1].

DDoS-атаки на DNS-сервери можна розділити на два класи. Атаки першого класу, котрі носять назву flooding-атак, переповнюють DNS-сервери великою кількістю DNS-запитів. Потік пакетів займає весь пропускний канал і не дає атакованій машині можливості обробляти легальні запити. Як правило, такі атаки виконуються шляхом зараження певного числа комп'ютерів відповідними програмами, котрі в певний момент починають здійснювати запити до атакованого сервера (рис.1).

Атаки другого класу експлуатують відкриті рекурсивні DNS-сервери, щоб більш наситити трафік, через який безпосередньо здійснюється атака, тому має назву DNS-атак з підсиленням. Відкриті рекурсивні сервери приймають DNS-запити навіть з чужих мереж та без будь-яких попередніх перевірок відправляють відповіді на задану IP-адресу. Ініціатори атаки заздалегідь замінюють її на IP-адресу «жертви». Коефіцієнт підсилення атаки може досягати значень з інтервалу 30…60. Тобто, на кожний умовний 1 байт запиту сервери відправлять 30…60 байтів відповіді «жертві». Відповідна схема атак такого класу зображена на рис. 2.

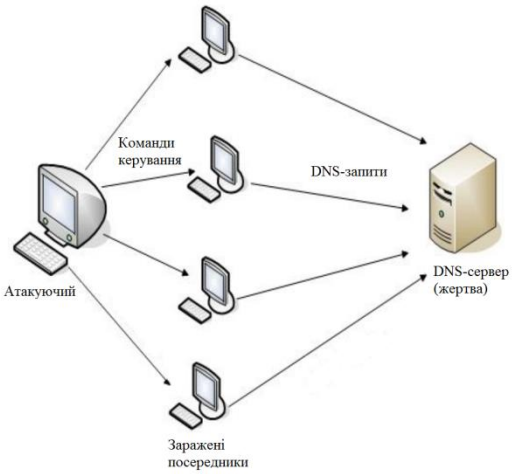

Рисунок 1. Архітектура flood-атаки

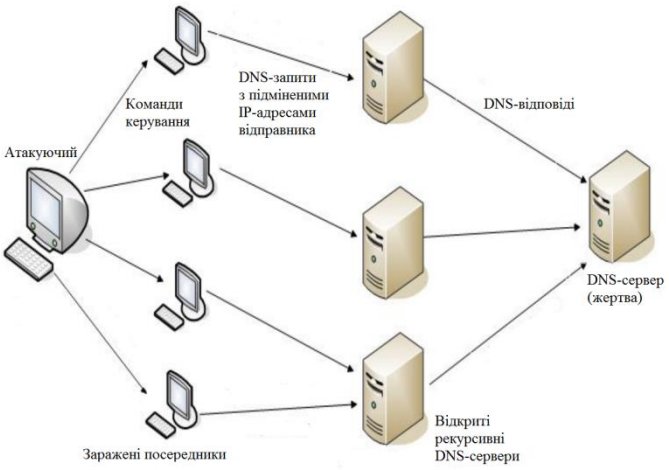

Рисунок 2. Архітектура DNS-атаки з підсиленням

Здебільшого, при виконанні flooding-атак використовується проміжна група з великої кількості заражених посередників. З іншого боку, «атакуючі» формують DNS-запити таким чином, щоб DNS-сервер не зміг знайти відповідну IP-адресу заданому доменному імені. Тобто, для трафіку DNS-сервера під час враження flooding-атаками притаманне високе значення відношення неуспішних спроб знаходження відповідності між доменним іменем та IP-адресою до успішних. Позначимо таке відношення за інтервал часу $\triangle t$ FSR:

$$FSR = \frac{\text{кількість неуспішних спроб}}{\text{кількість успішних спроб}}$$

Зазвичай, клієнт відправляє запит до свого локального DNS-сервера, а той у свою чергу, створює та надсилає відповідь. При DNS-атаках з підсиленням, DNS-сервер («жертва») отримує велику кількість відповідей без попередньої відправки відповідних запитів. Тобто, високе значення відношення кількості отриманих відповідей до отриманих запитів є характерною ознакою DNS-атак з підсиленням. Відношення відповідних пакетів за інтервал часу $\triangle t$ позначимо USQ:

$$USQ = \frac{\text{кількість отриманих відповідей}}{\text{кількість отриманих запитів}}$$

Узагальнену характеристику трафіку визначимо як зважену суму FSR та USQ і позначимо CAT:

$$CAT = \lambda USQ + (1-\lambda)FSR,$$

де $\lambda \in (0;1)$. Отже, flooding-атаки збільшуватимуть значення FSR, а DNS-атаки з підсиленням – значення USQ, при атаках кожного класу збільшуватиметься значення CAT. Таким чином, раптове збільшення CAT за короткий проміжок часу може сигналізувати про спробу DDoS-атаки на деякий сервер.

Обчислюючи значення CAT трафіку DNS-сервера на кожному часо-

вому проміжку $\triangle t$, можна сформувати часовий ряд CAT_i, $i = 1, 2, ...$ [2, 3]. Для моделювання такого часового ряду доцільно використовувати AAR(p) – адаптивну авторегресію порядку p:

$$a_i = \sum_{j=1}^{p} \phi_j(i) a_{i-j} + \varepsilon_i ,$$

де a_i − виміряні значення CAT на інтервалі $(i\triangle t; (i+1)\triangle t)$; $\phi_j(i)$ − параметри моделі; ε_i − білий шум (засоби моніторингу вимірюють параметри трафіку з похибками). Позначимо ваговий вектор $\phi(i) = [\phi_1(i), \phi_2(i), ..., \phi_p(i)]^T$. Ваговий вектор можна знайти за допомогою рекурсивного методу найменших квадратів, що дозволяє застосування цього підходу у режимі реального часу.

Багатовимірний ваговий вектор $\phi(i)$ розмірності p може бути використаний для відображення поточного стану DNS-трафіку. Раптова зміна значень CAT за короткий проміжок часу, що є характерною ознакою DDoS-атаки на DNS-сервери, відобразиться на ваговому векторі. Отже, всю множину можливих вагових векторів можна розділити на дві частини, одна з яких відповідає штатній роботі DNS-серверу, а інша − ймовірній DDoS-атаці на сервер. Тоді виявлення DDoS-атак зводиться до встановлення класу чергового вагового вектору – задача класифікації векторів. Для вирішення такої задачі доцільним буде використання методу опорних векторів.

Перелік посилань

1. Mirkovic J. Internet Denial of Service: Attack and Defense Mechanisms / J.Mirkovic, S.Dietrich, D.Dittrich. - Prentice Hall, 2005. – 400 с.

2. Бідюк П. І. Аналіз часових рядів: навчальний посібник / П.І.Бідюк, В.Д.Романенко, О.Л.Тимощук. – К. : Політехніка, 2010. – 317 с.

3. Cristianini N. An Introduction to Support Vector Machines and Other Kernel-based Learning Methods / N.Cristianini, J.Shawe-Taylor. - Cambridge University, 2000. – 204 с.

Анотація

Представлено метод виявлення DDoS-атак на DNS-сервер (flooding-атак та DNS-атак з підсиленням) з використанням часового ряду узагальненої характеристики його трафіку, який дозволяє проводити відстеження у режимі реального часу.

Ключові слова: DDoS-атаки, DNS-сервер, безпека мережі.

Аннотация

Представлен метод выявления DDoS-атак на DNS-сервер (flooding-атак и DNS-атак с усилением) с использованием временного ряда обобщённой характеристики его трафика, который позволяет проводить отслеживание в режиме реального времени.

Ключевые слова: DDoS-атаки, DNS-сервер, безопасность сети.

Abstract

An approach for detection of DDoS-attacks against DNS-server (flooding-attacks and DNS amplification attacks) using time series of generalized characteristic of its traffic which allows the monitoring in real time is provided.

Keywords: DDoS-attacks, DNS-server, network security.