УДК 621.39

ЗАХИСТ ТРАНСПОРТНИХ МЕРЕЖ ВІД DDoS АТАК

Гаттуров В.К., Шаповалов Р.С.
НТУУ «КПІ» Інститут телекомунікаційних систем
E-mail: sharom94@gmail.com

Protection transport network from DDoS attacks

The article describes the main types of DDoS-attacks and how they affect the transport network provider of telecommunications services. The article also describes some of the main methods to combat DDoS-attacks, and explained what effect do these methods to suppress the attacks.

Розподілені мережеві атаки часто називають атаками типу «відмова в обслуговуванні» (Distributed Denial of Service, DDoS). Успіх атак цього типу зумовлений обмеженням пропускної здатності, яка є однією з характеристик будь-якого мережевого ресурсу, наприклад інфраструктури. Під час DDoS-атаки ресурсу надсилається велика кількість запитів із метою вичерпати його можливості обробки даних і порушити нормальне функціонування.

Мережеві ресурси (наприклад, веб-сервери) завжди мають обмеження щодо кількості одночасно оброблюваних запитів. Крім обмеження потужності сервера, канал, яким сервер зв'язується з Інтернетом, також має скінченну пропускну здатність. Якщо число запитів перевищує граничні можливості якого-небудь компонента інфраструктури, можуть виникнути такі проблеми з рівнем обслуговування:

- формування відповіді на запити відбувається значно повільніше, ніж зазвичай,
- деякі або навіть всі запити користувачів можуть залишитися без відповіді.

Зазвичай кінцева мета зловмисника – цілковите припинення нормальної роботи веб-ресурсу, цілковита «відмова в обслуговуванні».

Атаки можна класифікувати за наступними ознаками:

а) За характером впливу (пасивний вплив, активний вплив),

б) По меті впливу (порушення конфіденційності інформації або ресурсів системи, порушення цілісності інформації, порушення працездатності (доступності) системи),

в) За умовою початку здійснення впливу (атака на запит від об'єкта що атакується, атака по настанню очікуваної події на об'єкті що атакується, безумовна атака),

г) За наявності зворотнього зв'язку з атакуючим об'єктом (зворотнім зв'язком, без зворотнього зв'язку (односпрямована атака)),

д) По розташуванню суб'єкта атаки щодо об'єкта який атакується (внутрішньо сегментний, міжсегментний),

е) За рівнем еталонної моделі ISO / OSI, на якому здійснюється вплив (фізичний, канальний, мережевий, транспортний, сеансів, представницький, прикладної).

Атаки в транспортних мережах.

В транспортних мережах DDoS атаки розглядаються на двох рівнях моделі OSI, а саме це L2 (Канальний) та L3 (Мережевий).

На L2 DDoS атаки це — «забивання» каналу. Це атаки, які спрямовані на позбавлення доступу до зовнішньої мережі внаслідок вичерпання канальної ємності. Абсолютно неважливо, яким саме чином. Як правило, для цієї мети використовуються масовані, з точки зору трафіку, атаки типу «що-небудь»-Amplification (NTP-, DNS, RIP-… Amplification може бути будь-який, не має сенсу перераховувати). Взагалі, до цього класу атак відносяться всілякі flood-и, в тому числі ICMP Flood і т.д. Основне завдання полягає в тому, щоб в канал розміром, скажімо, 1 Гігабіт/с залити хоча б 1,1 Гігабіт/с. Цього буде достатньо для припинення доступу.

На L3 DDoS атаки це — порушення функціонування мережевої інфраструктури. До цього класу відносяться, серед іншого, атаки, що приводять до проблем з маршрутизацією в рамках протоколу BGP, з анонсами мереж (Hijacking) — або атаки, наслідком яких стають проблеми на транзитному мережевому обладнанні: наприклад, переповнення таблиці відстеження сполук. Атаки даного класу відрізняються великою різноманітністю.

Захист від атак.

В залежності від типу атаки та рівня моделі OSI використовуються різні методи захисту від DDoS атаки.

На рівні L2, якщо смуга атаки перевищує 100 Гігабіт/с, то ці гігабіти потрібно десь обробляти, наприклад, на стороні провайдера або датацентру, і проблема завжди буде в «останньої милі». За допомогою технології BGP Flow Spec можна фільтрувати частина атак по сигнатурах пакетів — скажімо, Amplification легко відсікається по порту джерела. Однак подібний спосіб досить дорогий і не від всього здатний захистити.

На рівні L3 необхідно аналізувати мережеву інфраструктуру, причому не тільки свою. Одним з прикладом атак є BGP Hijacking. На жаль, автоматично з подібною напастю боротися неможливо, все доведеться робити вручну. Але до того, як почнеться боротьба, ще потрібно буде визначити, що дана проблема (крадіжка префікса) взагалі виникла. Якщо це сталося, то необхідно звернутися до мережного оператора, до адміністрації датацентру, до хостеру і т. д. Вони допоможуть у вирішенні проблеми. Але для цього потрібна просунута

аналітика мережевої інфраструктури, тому що ознакою Hijacking служить, в загальному випадку, тільки те, що, починаючи з якогось моменту, анонси даної мережі в інтернеті пішли «нетипові», не такі, як були протягом тривалого часу до цього. Відповідно, для своєчасного виявлення необхідно мати, як мінімум, історію анонсів.

Якщо у вас своєї автономної системи (AS) немає, то можна вважати, що боротьба з атаками на цьому рівні більш-менш є обов'язком вашого датацентру (або провайдера). Проте, заздалегідь зазвичай не можна сказати, наскільки той чи інший датацентр серйозно підходить до даної проблеми.

Існує декілька методів боротьби з DDoS атаками:

- На рівні вузла (повинен бути доступ до вузла через інший шлях);
- На рівні мережі (блокується все що може дати більше інформації про вас атакуючому(ping, traceroute));
- На рівні провайдера (аналіз пакетів та блокування підозрілих ip-адрес);
- На рівні обладнання операторів зв’язку (використання обладнання, котре може полегшити боротьбу з атаками внаслідок вбудованих функцій);
- На рівні адміністратора (можливість визначити джерело атаки та спробувати йому завадити);
- Комбінований (використання всіх можливих систем).

Висновки. Проведений аналіз показав, що DDoS атаки поводяться по різному в залежності від рівня моделі OSI та типу атаки. Основними методами захисту та боротьби проти таких атак являється обробка трафіку, який генерується під час атаки, відсіканя такого трафіки чи створення певних Firewall на обладнанні.

Можна сказати, що всі перераховані вище методи не покривають і 70% всіх методів боротьби з DDoS атаками і над цією темою, боротьби з DDoS атаками, працює досить багато людей у всьому світі.

Література

1. Атака через INTERNET / Медведовский И.Д., Семьянов П.В., Платонов В.В.;Под ред. проф. Зегжды П.Д. - СПб: Мир и семья-95, 1998. - 296с.
2. Защита информации в компьютерных системах и сетях [Текст] / Романец Ю.В., Тимофеев П.А. / Под ред. Шаньгина В.Ф. - М.: Радио и связь, 2001. - 376 с.
3. http://www.internet-technologies.ru/articles/article_436.html.