УДК 621.391

ДОСЛІДЖЕННЯ ЕФЕКТИВНИХ МЕТОДІВ БОРОТЬБИ З НАЙБІЛЬШ ПОШИРЕНИМИ DDOS-АТАКАМИ

Шаповалов Р.С., Гаттуров В.К.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорськаго, Украина
E-mail: sharom94@gmail.com

Research effective methods to combat the most common DDOS-attacks

This article presents the main research ways of dealing with DDoS-attacks on transport networks, thus shows the reliability of these networks using these methods to combat the most common DDoS-attacks.

У разі, коли напад здійснюється відразу з декількох джерел, таку атаку називають «розподіленої» Distributed Denial of Service. Власне DDoS і є сьогодні найбільшою загрозою, оскільки єдине джерело DoS- атак всі сучасні системи безпеки вже давно навчилися виявляти і блокувати. Проблема ускладнюється тим, що організувати DDoS можна швидко і недорого [2].
Ситуація з DDoS-атаками в Україні вкрай невтішна, ми спостерігаємо зростання їх кількості з кожним роком. Це відзначають багато аналітичні компанії, фахівці в області інформаційної безпеки, а також самі замовники, котрі все частіше стикаються з тим чи іншим видом мережевих погроз. Якщо раніше ці загрози були здебільшого загальними і пізнаваними, то зараз атаки значно еволюціонували і придбали цілеспрямований, точковий характер. DDoS-атак - найбільш поширена та заснована на ідеї флуду, тобто завалювання жертви величезною кількістю пакетів. Флуд буває різним: ICMP-флуд, SYN-флуд, UDP-флуд і HTTP-флуд. Сучасні DoS-боти можуть використовувати всі ці види атак одночасно, тому слід заздалегідь подбати про адекватну захист від кожної з них.

1. ICMP-флуд

Дуже примітивний метод забивання смуги пропускання і створення навантажень на мережевий стек через монотонну посилку запитів ICMP ECHO (пінг). Легко можна знайти за допомогою аналізу потоків трафіку в обидві сторони: під час атаки типу ICMP-флуд вони практично ідентичні. Майже безболісний спосіб абсолютного захисту заснований на відключення відповідей на запити ICMP ECHO або за допомогою брандмауера [1].

2. SYN-флуд

Один з поширених способів не тільки забити канал зв'язку, але і ввести мережевий стек операційної системи в такий стан, коли він вже не зможе приймати нові запити на підключення. Заснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через посилку SYN-пакета з

неіснуючим зворотною адресою. Після декількох спроб відіслати відповідь ACK-пакет на недоступний адрес, більшість операційних систем ставлять невстановлене з'єднання в чергу. І тільки після n-ої спроби закривають з'єднання. Так як потік ACK-пакетів дуже великий, незабаром чергу виявляється заповненою, і ядро дає відмову на спроби відкрити нове з'єднання. Найбільш розумні DoS-боти ще й аналізують систему перед початком атаки, щоб слати запити тільки на відкриті життєво важливі порти. Ідентифікувати таку атаку просто: досить спробувати підключитися до одного з сервісів. Оборонні заходи зазвичай включають в себе:

• Збільшення черги «напіввідкритих» TCP-з'єднань.

• Зменшення часу утримання «напіввідкритих» з'єднань.

• Включення механізму TCP syncookies.

• Обмеження максимального числа «напіввідкритих» з'єднань з однієї IP до конкретного порту [2].

3. *UDP-флуд*

Типовий метод захаращення смуги пропускання. Заснований на нескінченній посилці UDP-пакетів на порти різних UDP-сервісів. Легко усувається за рахунок відрізання таких сервісів від зовнішнього світу і установки ліміту на кількість з'єднань в одиницю часу до DNS-сервера на стороні шлюзу [2].

4. *HTTP-флуд*

Один з найпоширеніших на сьогоднішній день способів флуду. Заснований на нескінченній посилці HTTP-повідомлень GET на 80-й порт з метою завантажити web-сервер настільки, щоб він виявився не в змозі обробляти всі інші запити. Часто метою флуда стає корінь web-сервера, а один з скриптів, що виконують ресурсомісткі завдання або працює з базою даних. У будь-якому випадку, індикатором почалася атаки служитиме аномально швидке зростання податків web-сервера.

Методи боротьби з HTTP-флудом включають в себе тюнінг web-сервера і бази даних з метою знизити ефект від атаки, а також відсіювання DoS-ботів за допомогою різних прийомів. По-перше, слід збільшити максимальну кількість конектів до бази даних одночасно. По-друге, встановити перед web-сервером Apache легкий і продуктивний nginx - він буде кешувати запити і віддавати статику. Це рішення зі списку «must have», яке не тільки знизить ефект DoS-атак, але і дозволить сервера витримати величезні навантаження [2].

У разі необхідності можна задіяти nginx-модуль ngx_http_limit_req_module, що обмежує кількість одночасних підключень з однієї адреси. Ресурсомісткі скрипти можна захистити від ботів за допомогою затримок, кнопок «Натисни мене», виставлення кукисов і інших прийомів, спрямованих на перевірку «людяності».

Надалі розглянемо універсальні поради, *щ*об не потрапити в безвихідне становище під час обвалення DDoS-шторму на системи, необхідно ретельно підготувати їх до такої ситуації:

1. Всі сервера, що мають прямий доступ в зовнішню мережу, повинні бути підготовлені до простого і швидкого віддаленого ребуту. Великим плюсом буде наявність другого, адміністративного, мережевого інтерфейсу, через який можна отримати доступ до сервера в разі затурканості основного каналу. Перевагою буде також перенесення роботи sshd зі стандартного порту на будь-який інший [3].

2. ПО, що використовується на сервері, завжди має перебувати в актуальному стані. Всі дірки - пропатчити, поновлення встановлені (простий, як чобіт, рада, якій багато хто не йдуть). Це захистить тебе від DoS-атак, що експлуатують баги в сервісах.

3. Всі, хто слухає мережеві сервіси, призначені для адміністративного використання, повинні бути заховані брандмауером від усіх, хто не повинен мати до них доступ. Тоді атакуючий не зможе використовувати їх для проведення DoS-атаки або брутфорса [4].

4. На підходах до сервера (найближчому маршрутизаторі) повинна бути встановлена система аналізу трафіку (NetFlow в допомогу), яка дозволить своєчасно дізнатися про початок атаки і вчасно вжити заходів по її запобіганню.

Висновки. Масштаби і руйнівна сила атак DDoS продовжують рости, оскільки застосовуються все більш потужні і легкодоступні інструменти атаки, в мережі Інтернет багато вразливих точок, і росте «Інтернет-залежність» компаній. Оскільки збиток від таких атак збільшується, провайдери, компанії та урядові відомства повинні застосовувати відповідні заходи для захисту своїх інвестицій, доходів і послуг. Тут потрібно рішення нового типу, яке доповнило б існуючі рішення щодо забезпечення безпеки, зокрема, міжмережеві екрани і системи IDS, і могло не тільки виявляти найвитонченіші атаки DDoS, а й блокувати все більш витончений і важко вловимий трафік атак без шкоди для благонадійних транзакцій. При такому підході потрібно більш досконала, ніж в існуючих на сьогоднішній день рішеннях, перевірка і аналіз трафіку атаки, що підтверджують результати дослідження.

Література

1. David Dittrich, The "Tribe Flood Network" distributed denial of service attack tool, October 21, 1999.
2. Скудис Э. Противостояние хакерам. М.: ДМК Пресс, 2003. — 506 с. –с. 349-370.
3. Журнал Хакер. DDoS с умножением через DNS-резолверы: технические подробности.
4. Стивен Норткат, Джуди Новак. Обнаружение нарушений безопасности в сетях. Третье издание. Перевод с английского: Издательский дом «Вильямс», 2003 – 448 стр.