УДК 004

ВИКОРИСТАННЯ МАЛОІНТЕНСИВНИХ DDOS-АТАК ДЛЯ МАСКУВАННЯ ВТОРГНЕННЯ

А. С. Малишко[1, a], А. М. Кудін[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Дана робота присвячена властивості DDoS-атак блокувати роботу системи виявлення вторгнень та фаерволів. Розглянуті властивості малопотужних DDoS-атак та методи протидії ним.

Ключові слова: малоінтенсивні DDoS-атаки, інформаційна безпека, система виявлення вторгнень, DDoS

Вступ

Кожен рік DDoS-атаки ставлять нові рекорди. Значну роль у цій тенденції відіграє «інтернет речей», який значно розширився у останні роки. Атаки величезної потужності здатні обмежити користувачам доступ до сервісу, але небезпека полягає не тільки в цьому. Об'єми трафіку, який ботнети здатні генерувати одночасно, сягає 1.3 [1] терабіт на секунду, але забивання каналів фіктивним трафіком – не єдина загроза від DDoS-атак. Навіть короткі слабкі атаки можуть вивести систему запобігання вторгнень (IPS) або фаерволл з ладу [2], а цього достатньо для реалізації справжньої атаки – проникнення злочинних пакетів скрізь систему захисту.

1. Схеми захисту від DDoS-атак

На даний момент, найрозповсюдженішими є дві схеми захисту від DDoS-атак [3]:

1) Хмарна архітектура – за допомогою засобів третьої сторони;
2) Локальна архітектура – за допомогою власних засобів.

1.1. Хмарна архітектура

Для відбиття DDoS-атаки власної обчислювальної потужності сервера може бути недостатньо. У такому випадку є можливість підключити потужні сервери, побудовані спеціально для фільтрації трафіку – наприклад, такі рішення представляють компанії Cloudflare, Akamai та Arbor. Така міра дозволяє відбивати найпотужніші атаки, але вона вимагає до 10 хвилин часу (див. рис. 1).

Переваги:

- Можливість підключення потужності, достатньої для подолання атаки будь-якого обсягу
- Не потребує менеджменту: за всім наглядає провайдер

Недоліки

- Затримка від 5 до 15 хвилин для гарантованого виявлення атаки
- Необхідна тісна взаємодія з провайдером для регулювання параметрів сервісу
- Менше контролю

Використання хмарної архітектури захисту від DDoS-атаки передбачає перемикання трафіку на сервери провайдера у складній ситуації. У випадку, коли фаервол (або IPS) виходять з ладу до переключення, у хакерів залишається вікно для реалізації свого плану.

1.2. Локальна архітектура

Цей підхід полягає у використанні власних ресурсів для подолання загрози.

Переваги:

- Повний контроль над усією структурою
- Можливість вибору засобів захисту
- Незалежність від третьої сторони

Недоліки:

- Потребує адміністрування
- Залежність від встановленого обладнання
- Ціна

Можливим варіантом є встановлення обладнання, достатнього для блокування DDoS-атак середньої потужності. У цьому випадку для його подолання необхідно збільшити потужність атаки, а це збільшує імовірність її своєчасного виявлення.

2. Малоінтенсивні DDoS-атаки

DDoS-атаки можуть виступати не лише як метод блокування ресурсу, а і як маскування для інших більш небезпечних атак. При цьому порушити нормальну роботу фаервола здатен не лише високоінтенсивний флуд, а і слабкі атаки [4]. Вони можуть здаватися нешкідливими, бо не блокують роботу сайту на довгий час як повномасштабні атаки, та

[a] an.malyshko@gmail.com

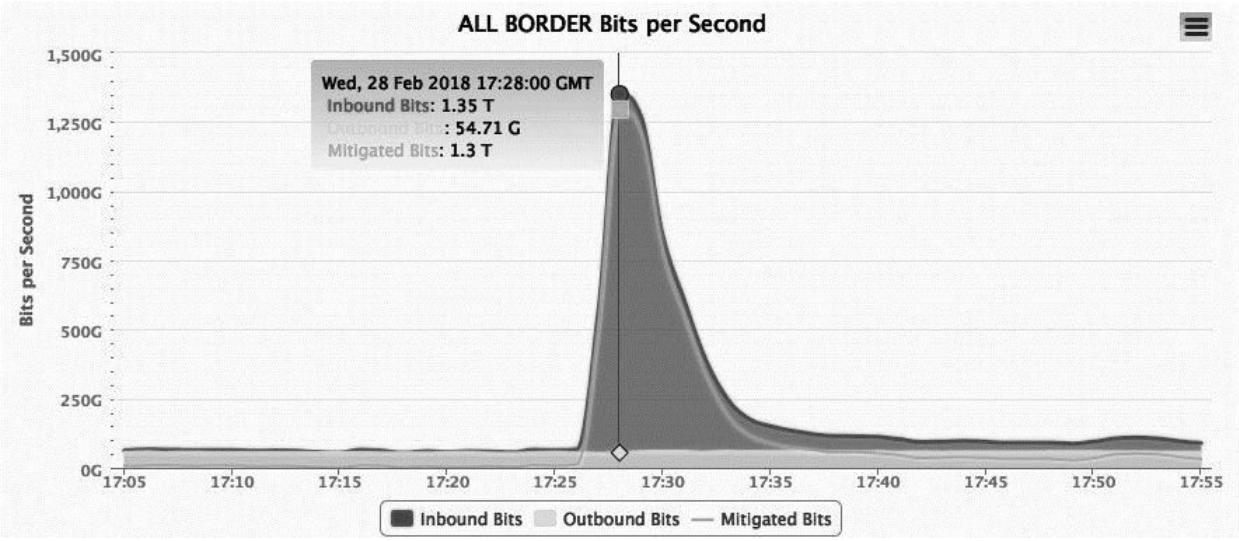

Рис. 1. Рекордна DDoS-атака на GitHub 28.03.2018

іноді залишаються непоміченими застарілими системами захисту [2]. Але ігнорування цієї загрорзи дає хакерам реальну можливість встановити злочинне програмне забезпечення у систему, компромітувати приватну інформацію [5], складати карту мережі та аналізувати внутрішній трафік.

3. Методи протидії

Досить ефективним рішенням для протидії скритним атакам є побудова на периметрі мережі багаторівневої системи захисту, яка представляє собою спеціалізоване рішення для боротьби з DDoS-атаками [6].

Основною причиною успіху DDoS-атак є непідготовленість цілі до них. Але це може трапитись з кожним. Тенденції останнього часу (в основному – зростання обсягу інтернету речей, IoT) полягають у збільшенні частоти цих атак та їх доступності: замовити DDoS-атаку стало дешево та легко, тому конкуренти можуть звертатися до такої можливості під час піку попиту.

Таким чином, необхідно впевнитись, що система є захищеною від загроз. Одним з ефективних рішень є моделювання загрози до її реалізації – наприклад, за допомогою сервісів тестування захищеності систем (наприклад, Ixia BreakingPoint та Radware TierPoint). Ці сервіси призначені для перевірки стійкості до різнотипових загроз за допомогою імітації реальної атаки та аналізу стану системи у процесі.

4. Висновки

Розглянуті факти та моделі дозволяють зробити висновок про необхідність комплексного захисту від різних видів DDoS-атак та його тестування на моделях можливих загроз. DDoS-атаки постійно еволюціонують, тому старі підходи перестають працювати. Необхідно використовувати новітні рішення від надійних поставників послуг.

Перелік використаних джерел

1. Зафиксирована самая мощная кибератака за всю историю интернета. — 2018. — Режим доступа: https://lenta.ru/news/2018/03/02/ddos/.
2. Short, Stealthy, Sub-Saturating DDoS Attacks Pose Greatest Security Threat to Businesses. — 2017. — Access mode: https://www.corero.com/company/newsroom/press-releases/short-stealthy-sub-saturating-ddos-attacks-pose-greatest-security-threat-to-businesses/.
3. Burke John. Defense for Distributed Denial of Service Attacks. — 2013. — Access mode: https://www.business.att.com/content/whitepaper/Nemertes-DN2400-ATT-DDos-Issue-Paper.pdf.
4. A potential low-rate DoS attack against network firewalls / Salah K., Sattar K., M. Sqalli, Ehab Al-Shaer. — 2011. — Access mode: https://doi.org/10.1002/sec.118.
5. Gibbs Samuel. TalkTalk criticised for poor security and handling of hack attack. — 2015. — Access mode: https://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack.
6. Murphy Tim. Don't rely on your firewall & IPS when it comes to preventing DDoS attacks. — 2017. — Access mode: https://www.cso.com.au/article/620372/don-t-rely-your-firewall-ips-when-it-comes-preventing-ddos-attacks/.