РІЗНОВИД DOS-АТАК ТА DDOS-АТАК

Рябчук А. Р.
студентки ІІІ курсу факультету права та економіки
Міжнародний гуманітарний університет
Слатвінська В. М.
викладач кафедри кримінального права, процесу та криміналістики
факультету права та економіки
Міжнародний гуманітарний університет
м. Одеса, Україна

Найбільш поширеними способами здійснення кібератак П. Нойман вважає сніфер пакетів та IP-спуфінг, DoS і DDoS атаки, парольні атаки, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки й так звані ін'єкції [1, с. 47]. Що таке DoS-атака? DoS означає відмову в обслуговуванні (Denial of Service). Зловмисник нападає з метою викликати перевантаження підсистеми, в якій працює сервіс, що атакується. Вплив здійснюється з одного сервера і націлений на певний домен або віртуальну машину.

Особливості DoS-атак:

- Одиночний характер - потік трафіку запускається з однієї-єдиної підмережі.

- Висока помітність - спроби «покласти» сайт помітні за вмістом лог- файлу.

- Простота придушення - атаки легко блокуються за допомогою брандмауера.

Останнє також часто покладається на мережеве обладнання, наприклад маршрутизатор, в якому встановлено полегшений варіант Linux або подібне програмне забезпечення. Такий тип атак давно не становить особливої небезпеки, але впливає на вартість обслуговування (вимагає встановлення спеціалізованих програм).

Що таке DDoS-атака? DDoS означає розподілений відмова в обслуговуванні (Distributed Denial of Service). Реалізується атака трохи інакше, ніж DoS - принципова відмінність полягає у застосуванні відразу кількох хостів. Складність захисту від цього виду нападу залежить від кількості машин, з яких здійснюється надсилання трафіку.

Особливості DDoS-атак:

* Багатопотоковий характер - такий підхід спрощує завдання блокування сайту, тому що швидко відсіяти всі атакуючі IP-адреси практично нереально.

* Висока скритність - грамотна побудова атаки дозволяє замаскувати її початок під природний трафік і поступово «забивати»

веб-ресурс порожніми запитами.

* Складність придушення - проблема полягає у визначенні моменту, коли атака почалася [1, с. 51].

Ручне дослідження лог-файлів тут нічого не дає, відрізнити хости, що атакують, від «нормальних» практично неможливо. Ситуація посилюється тим, що джерелом у 9 випадках з 10 виявляються «звичайні сайти», заражені вірусом або зламані вручну. Поступово вони утворюють єдину мережу, яку називають ботнетом, і збільшують потужність атаки.

Головні відмінності та цілі атак:

Найбільш поширена причина, чому хтось вирішує «покласти» веб-ресурс, полягає у здирстві. Система схожа із зараженням локальних комп'ютерів вірусами-здирниками, при активації яких з власника починають вимагати викуп за повернення працездатності Windows. Те саме відбувається з сайтом - хакер надсилає власнику email із вимогами.

Трапляються й інші причини:

* Несумлінна конкуренція - «колеги» намагаються зайняти нішу шляхом видалення інших гравців ринку.

* Розвага - молоді програмісти запускають атаки заради хвастощів перед друзями, знайомими, колегами.

* Неприязнь особистого, політичного характеру - мотивом стає незгоду з політикою уряду, певної організації.

Також можливі проблеми, що виходять від незадоволених співробітників, які звільнилися або ще продовжують працювати, але вже готові пакостити своєму роботодавцю.

Натомість спільною ознакою DoS і DDoS атак - змушення серверу стресувати й відсутність погодженості щодо початку стрес-тестування.

Література:

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015.- 288 с.