УДК 004.7
У. Яциковська, Я. Кінах
(Тернопільський національний технічний університет імені Івана Пулюя)

ВПЛИВ АТАК НА ВІДМОВУ В ОБСЛУГОВУВАННІ НА КОМП'ЮТЕРНІ МЕРЕЖІ

Серед численних атак зловмисників на комп'ютерні мережі найпоширенішими є переривання і спотворення пакетного трафіка. Найруйнівнішими атаками на сьогоднішній час є атаки, спрямовані на відмову в обслуговуванні легітимних послуг.

Згідно звіту даних компанії Prolexic, лідера світового ринку захисту від атак на відмову від обслуговування, середня потужність атаки становить 49 Гб/с, 17 % атак мають потужність більше 60 Гб/с. Відносний приріст середнього значення потужності складає 925 % або 1655 % пакетів за секунду [1]. Атаки низької потужності є цільовими рівня HTTP Flood або SYN Flood. Максимальна потужність використовується для захищених ресурсів комп'ютерної мережі. Атака знищує не лише сайт, а й весь хост та мережу провайдера. Таких атак із кожним роком стає все більше.

На практиці для мінімізації втрат від атаки використовують методи фільтрації UDP трафіка. Такий метод є ефективним для короткотривалого захисту автономних систем глобальної мережі за наявності сучасних засобів фільтрації у прикордонній частині мережі та керуванні висококваліфікованими спеціалістами. Такі програмно-апаратні комплекси є високовартісними та не виявляють ініціаторів атаки. На рисунку 1. показано завантаження засобу фільтрації під час реалізації реальної атаки на відмову в обслуговуванні [2].

Аналіз показав, що існуючі засоби захисту не справляються із керуванням трафіка шляхом фільтрації. Тому виникає гостра необхідність у створенні нових методів та засобів захисту архітектур типу клієнт-сервер від атак на відмову в обслуговуванні.

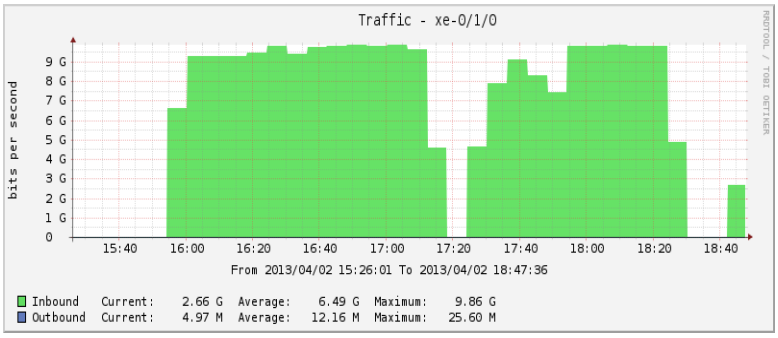

Рисунок 1 - Робота UDP – фільтру під час DDoS-атаки

Проаналізувавши підходи до методів відслідковування атак, виявлено, що для задачі трасування IP-адрес перспективним методом є імовірнісне маркування пакетів. Цей підхід доцільно застосовувати під час атаки або після проведення атаки. В методі імовірнісного маркування пакетів не генерується додатковий мережевий трафік, а зберігається інформація про маршрутизатори чи збільшується розмір пакета.

Для відстеження IP-адреси ініціатора атаки на відмову в обслуговуванні доцільно використати метод імовірнісного маркування пакетів. Відомо, що в даному методі кожен маршрутизатор імовірнісно вписує свою локальну інформацію про шлях проходження пакету до кінцевого вузла. Отже, користувач із високою імовірністю може відновити повний шлях проходження пакетів, перевіряючи маркування. У алгоритмі імовірнісного маркування пакетів кожен маршрутизатор випадково визначає імовірність маркування, який перезаписує інформацію в полі маркування, знищуючи маркування пройдених маршрутизаторів.

1. Ioannidis J. Implementing pushback: Router-based defense against DDoS attacks / J. Ioannidis, S.M. Bellovin // In proceedings of network and distributed system security symposium : The Internet Society, 2002. : thesis. – 2002. – P. 26–38.

2. Burch H. Tracing anonymous packets to their approximate source / H. Burch, B. Cheswick // In Usenix LISA Conference : thesis. – New Orleans., 2000. – P. 313– 322.