УДК 004.056 :004.62

ДОСЛІДЖЕННЯ DDOS-АТАК ЗА 2015 РІК

Войтович О.П.,
к.т.н., доцент,
доцент кафедри захисту інформації,
Вінницький національний технічний університет,
voytovych.op@gmail.com

Хомін Д.М.,
магістрант кафедри захисту інформації,
Вінницький національний технічний університет,
dima.khomin@gmail.com

Анотація. *У роботі проведено аналіз DDos-атак за останні роки. Виявленні тенденції як зростання типових атак типу HTTP-flood, так і появи нових видів атак.*

В останні роки DDoS-атаки отримали репутацію найбільш грізної кібернетичної зброї і були взяті на озброєння різноманітними Інтернет-зловмисниками, починаючи від новачків та скріпт-кіддерів завершуючи організованими злочинними групами та спеціалізованими організаціями. DDoS-атака як один з найбільш недорогих і надійних способів тиску на жертву використовується і в конкурентній боротьбі, і для банального шантажу компаній, бізнес яких побудований на web-сервісах, і в політичній боротьбі (рідкісні вибори в розвинених країнах сьогодні обходяться без DDoS-атак на сайти противників), і в кібервійнах (наприклад атаки на об'єкти електропостачання в Україні), і просто для «завалу» будь-яких важливих ресурсів. І, треба відзначити, прибутковість цього кримінального бізнесу досить велика.

За перше півріччя 2015 року, малий та середній бізнес в ході DDos-атак втратив 52000 $, а великий бізнес втратив 444000 $. 26 % компаній зіткнулись з підвищенням страхування, 29% - втратили позиції в кредитних рейтингах, 33% - втратили бізнес можливості, 38% - тимчасово призупинили власну діяльність та 63% - втратили доступ до важливої для бізнесу інформації. Здебільшого DDos-атаки почастішали на такі Інтернет-ресурси як платіжні системи (порівняно з 2014 роком на 582%), соціальні мережі (на 647%), сайти банків та нерухомості (на 230%). Зменшилась кількість атак в порівняні з 2014 роком на Інтернет-ресурси ЗМІ та бірж [1].

Аналіз статистики кіберзлочинів за 2015 рік [2] показав, що DDos-атаки завжди входять в п'ятірку лідерів. В середньому їх відсоток коливається на рівні 10%. Дослідивши статистику за минулі роки [3], можна побачити зростаючу тенденцію відсотка цих атак у кіберзлочинах (рис. 1).

В основі майже всіх атак DDoS лежить один і той же механізм, коли велика кількість хостів посилають запити на одну і ту ж адресу мережного ресурсу. Лавиноподібне зростання трафіку виводить з ладу або просто перевантажує сервер, на який адресуються запити. Всі DDoS-атаки так чи інакше спрямовані на виснаження системних ресурсів.

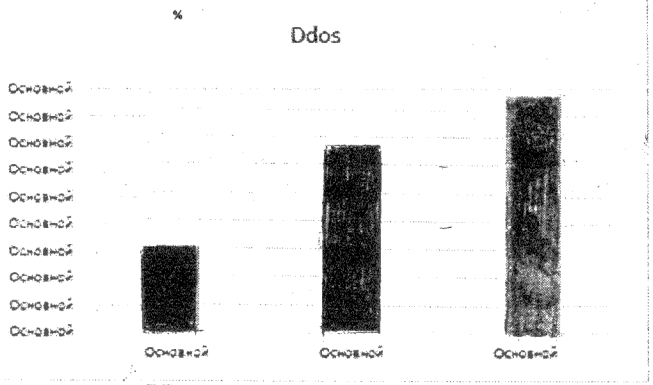

Рис. 1. Відсоткова частка DDos-атак серед загальної кількості кібератак за 2013-2015 рр.

За даними Лабораторії Касперського [3] найбільш популярним видом атаки є HTTP Flood (80%), коли на сайт що атакується одночасно відправляється низка HTTP-запитів. Зловмисники використовують різні технології проведення атак цього типу. У 55% випадків атак типу HTTP Flood боти намагаються звернутися до якоїсь однієї сторінки сайту; на другому місці з показником 22% знаходяться атаки на різні форми авторизації; третє місце (12%) зайняли атаки з використанням численних спроб скачування будь-якого файлу з сайту. І лише в одному випадку з 10 проводяться більш складні атаки, коли зловмисники намагаються замаскувати дії ботів під поведінку справжніх користувачів. На другому місці з показником 10% розташувалися атаки типу UDP Flood. Боти, що здійснюють такі атаки, покладаються на «грубу силу», тобто генерують велику кількість досить невеликих за розміром (наприклад, по 64 байти) пакетів. На третьому і четвертому місцях у рейтингу популярності у зловмисників стоять атаки типу SYN Flood (8%) і ICMP Flood (2%) відповідно. Діаграма показана на рис. 2.

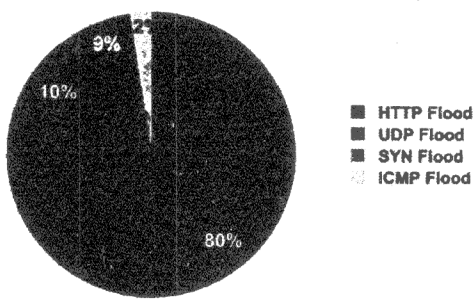

Рис. 2 – Діаграма розповсюджених DDoS-атак

У 2015 році з'явився новий тренд – атаки на інфраструктуру мережі (маршрутизатори, комутатори), у тому числі маніпуляції з протоколами маршрутизації. Такі атаки впливають не на додатки або канали, а на інформацію про маршрути, працездатність обладнання, яке пересилає пакети. У цьому напрямку буде зміщуватися фокус атак в найближчі кілька років, оскільки з атаками на смугу пропускання,

наприклад, вже навчилися боротися. А атаки, що впливають на інфраструктуру мережі, вкрай руйнівні, оскільки їх складно виявити, і методи протидії тільки починають розроблятися [4].

Знову з'явилася тенденція щодо збільшення числа DDoS-атак на веб-додатки на сьомому рівні мережевої моделі OSI з використанням класичних ботнетів. Якщо раніше ботнети використовувалися в основному для розсилання спаму, майнінгу криптовалюти та виконання примітивних DDoS-атак, то сьогодні вони прогнозовано стають все більш серйозною загрозою безпеці [4].

Отож, проаналізувавши звіти різних провідних компаній з протидії Інтернет-злочинам, можна зробити висновок, що DDos-атаки стають більш актуальними та спричинюють серйозні загрози як бізнесу, так і державній безпеці.

Література:

1. 2015 Cyber Attacks Statistics – 2016. – Режим доступу до статті: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/

2. Основная статистика за 2015 год – 2016 – Режим доступу до статті: https://kasperskycontenthub.com/securelist-russia/files/2015/12/KSB_2015_Stats_FINAL_RU

3. Компьютерная сеть и ботнеты // [Электронный ресурс]. – Режим доступа: http://alsiti.net/index.php?topic=396.0

4. Исследование DDoS-атак и уязвимостей в веб-приложениях в первой половине 2015 года – 2015 – Режим доступу до статті: http://qrator.net/ru/company/news/issledovanie-ddos-atak-i-uiazvimostei-v-veb-prilozheniiakh-v-pervoi-polovine-2015-goda