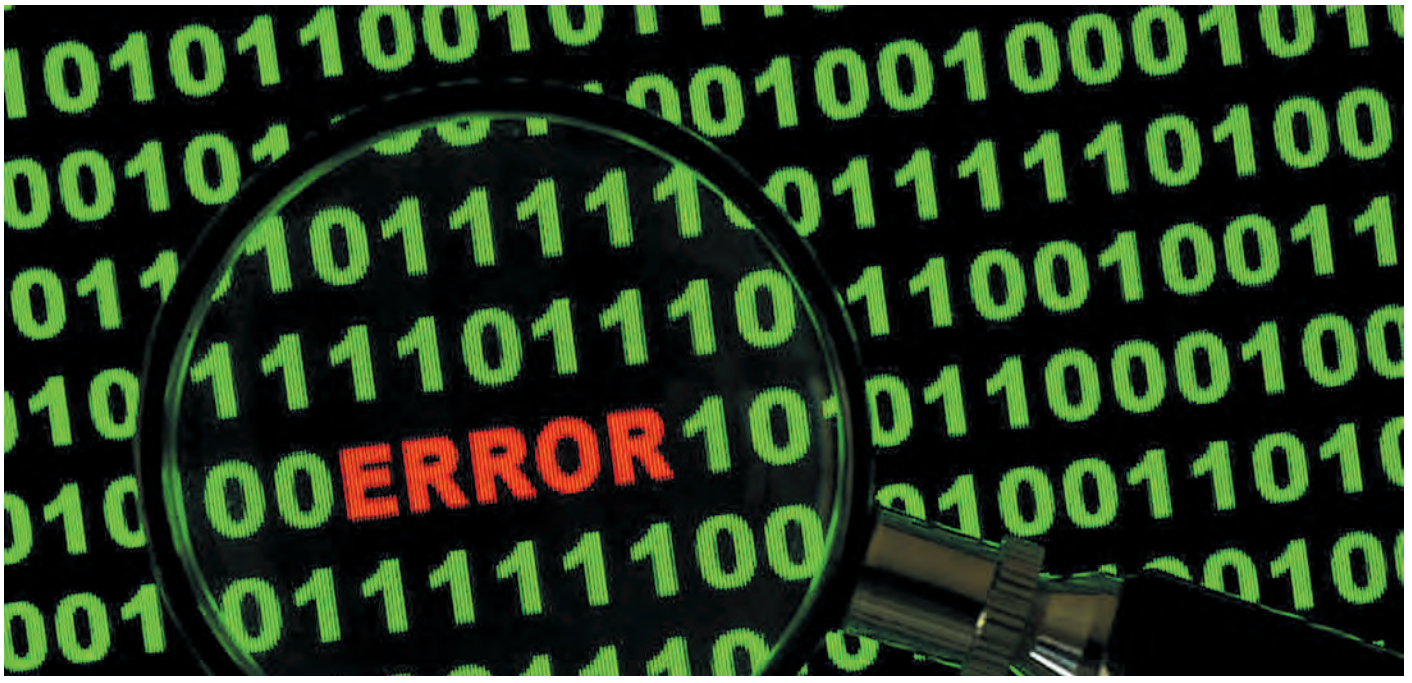
DDoS-атаки і захист від них



Про цей вид кібератак ми й так не забували, але в умовах війни почалося їх масове застосування.

DDoS-атаки — явище дуже давнє, проте так само дошкульне і небезпечне. У цій сфері, як і загалом у кіберзлочинності, відбувається здешевлення атак, вони стають більш доступними і водночас загрозливими. Сприяє цьому цифрова трансформація, оскільки об'єктами атак стають хмари, пристрої IoT і мережі мобільного зв'язку. Останнім часом DDoS-атаки використовуються для здирництва як додатковий важіль впливу.

Ще до початку російського вторгнення Україна зазнала потужних DDoS-атак, продовжились вони і з відкритим початком бойових дій, причому не лише проти України, але і проти наших союзників.

Функцію анти-DDoS мають сучасні мережеві екрани, існують і спеціалізовані рішення, здатні відбивати найпотужніші атаки. Захист від DDoS пропонують як послугу оператори телекомунікацій і компанії, що працюють у сфері кібербезпеки. «МтБ» розбирається у типах DDoS--атак і способах захисту від них.

Атакують з усіх боків

Якими бувають DDoS-атаки? Найпростіші об'ємні, або ж flood, їхнім завданням є перевантаження мережі потоком запитів, щоб заблокувати роботу веб– або DNS-сервера. При цьому пакети запитів навіть не обов'язково повинні бути коректними: важливо, аби вони дісталися потрібної адреси. Існує багато типів flood-атак, які використовують слабкі місця у мережевих протоколах або неналежне налаштування обладнання. Наприклад, атаки типу ACK і SYN перевантажують сервер, експлуатуючи процедуру рукостискання під час встановлення TCP-з'єднання. В атаках типу DNS flood сервер DNS перевантажується запитами на конвертацію адрес.

Сама атака часто здійснюється через бот-мережу (ботнет), що складається з заражених комп'ютерів і діє за вказівками сервера управління. Останніми роками для цього все частіше використовуються пристрої Інтернету речей, які є дуже численними, відносно потужними

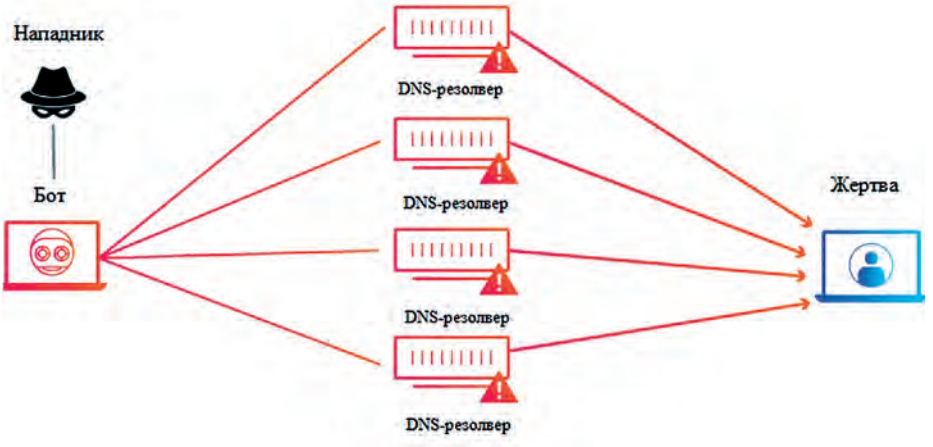


Рис. 1. Схема DDoS-атаки типу «посилення/відображення» з використанням DNS (джерело: Cloudflare)

(як, наприклад, IP-камери) і некерованими, при тому що часто вони мають вразливості, які виробники закривають дуже повільно або взагалі їх ігнорують. Саме через IoT у 2016 році було здійснено першу відому атаку Mirai.

Мета атак типу «посилення/відображення» (amplification/reflection) — простим запитом спровокувати сервер або інший пристрій генерувати великий об'єм трафіку в напрямку жертви. Найчастіше використовується вразливість протоколу UDP, який зазвичай використовується для обміну DNS: а саме що для пришвидшення операцій DNS-сервер не верифікує джерела запитів. При цьому, надсилаючи короткі запити і отримуючи об'ємні відповіді, можна згенерувати значний потік трафіку. Зловмисник, отже, надсилає пакети на сервер DNS, а той відправляє відповіді на IP-адресу жертви (**рис. 1**). В Інтернеті можна зустріти різні аналогії цьому явищу; наприклад, ***Cloudflare*** наводить такий приклад, ніби підліток-хуліган телефонує до ресторану, замовляє все меню і просить йому передзвонити і перелічити все замовлення. Коли ж ресторан запитує, куди саме передзвонити, він називає номер жертви, якій відповідно телефонують і зачитують інформацію, якої вона не просила.

DDoS-атаки прикладного рівня вимагають знання відповідних програм і застосунків, але не потребують таких великих об'ємів трафіку, як мережеві. Ботнет завалює сервер зверненнями: в атаках типу HTTP GET він відправляє запити на отримання контенту, а HTTP POST — навпаки, намагається надсилати дані для заповнення веб-форми, що вимагає їхньої обробки й занесення до бази даних. Порівняно з мережевими, атаки прикладного рівня складно відбивати: оскільки кожен бот робить на позір легітимні запити, і трафік видається цілком нормальним.

«Малі і повільні» атаки («low and slow») завантажують веб-сервери таким чином, щоб справжні користувачі не мали до них доступу. Це досягається шляхом надсилання даних у дуже повільному темпі, але все ж достатньо швидко, щоб з'єднання не переривалося через вичерпання часу. Наприклад, один з інструментів для таких атак надсилає HTTP-заголовки невеликими частинами, інший робить POST-запит, зазначаючи, якого об'єму даних чекати, але відправляє ті дані дуже повільно. Атаки «low and slow» теж важко виявляти, оскільки їхній трафік незначний і цілком легітимний. Окрім того, оскільки такі атаки не потребують великих ресурсів, їх можна запускати навіть з одного комп'ютера.

DDoS-атаками, звісно, займаються кіберзлочинці, причому існує ціла індустрія виконання таких атак на замовлення. Як свідчить компанія ***A10***, це досить конкурентний ринок з гарним клієнтським сервісом (зокрема, якщо атакована ціль не «падає», замовнику можуть повернути гроші). Часто атака відбувається автоматично, так що замовник і виконавець навіть не контактують між собою.

Злочинці також не гребують DDoS-атаками для вимагання викупу, погрожуючи заблокувати роботу компанії, якщо з ними не розплатяться. Для демонстрації своїх можливостей вони можуть запускати обмежені атаки з метою «покласти» сайт на обмежений період часу, щоб потім вимагати грошей за уникнення масштабнішої атаки.

Доступність інструментів для DDoS робить цей вид атак зручним засобом не лише для злочинців, а й для будь-кого, хто бажає самоствердитися або помститись кому-небудь. Починаючи від онлайн-хуліганів (script kiddies, як їх називають на Заході) до хакерів, які атакують відомі сайти, аби здобути престиж у середовищі собі подібних. Як до виду помсти до DDoS-атак можуть вдаватись незадоволені покупці або звільнені працівники, які мають зуб на колишню компанію. Відомі випадки, коли атаки здійснюються не групами хакерів, а одним користувачем проти іншого. Особливо це поширено серед тих геймерів, які

витрачають на ігри багато часу і грошей, а тому іноді можуть вдаватися до спроб фізично заблокувати суперника.

Вдаються до DDoS-атак і різноманітні хактивісти, які таким чином заявляють про ту чи іншу політичну позицію. Найвідомішою з таких груп є Anonymous, але з початком широкомасштабного вторгнення РФ в Україну хактивізм, вибачте за каламбур, значно активізувався.

Нарешті, користуються цим інструментом і групи хакерів, афілійовані з державними органами, про що українцям відомо як нікому іншому. DDoS-атаки часто використовуються для відвертання уваги і замітання слідів справжньої хакерської кампанії.

Статистика DDoS

Як виглядає ландшафт атак станом на зараз? Компанії, які пропонують технічні рішення та послуги з відбиття DDoS, на основі результатів власної роботи складають регулярні звіти, щоквартальні або піврічні, де наводять статистику і динаміку загроз.

Зокрема, Cloudflare у своєму звіті за 1-й квартал 2022 року, відштовхуючись від результатів власних вимірювань, стверджує, що порівняно з таким же періодом минулого року кількість атак мережевого рівня зросла на 71%. При цьому порівняно з минулим кварталом різко підскочило число об'ємних атак: понад 10 Мпс (мільйонів пакетів на секунду) — утроє, понад 100 Гпс — на 645%. Загалом майже 90% DDoS-атак мають розмір менш ніж 50 кпс, чого, втім, достатньо, щоб обвалити незахищений сервер і навіть частково перекрити стандартне з'єднання Gigabit Ethernet. Середня швидкість атаки також залишається нижчою за 500 Мбіт/с. Понад 90% атак тривали менше години: зокрема, у більш ніж половині випадків час

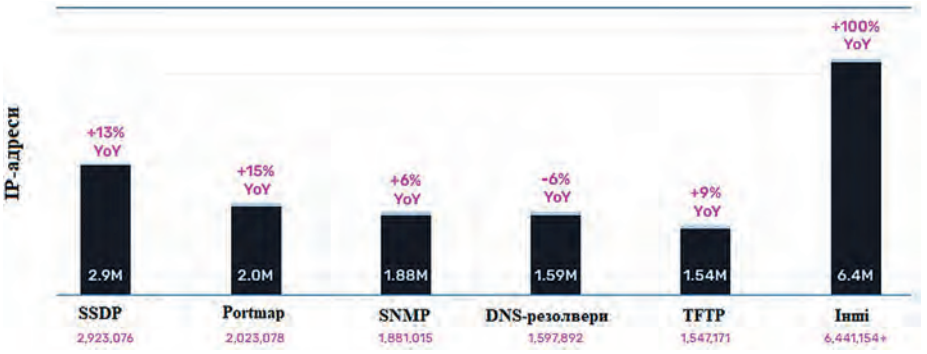


Рис. 3. DDoS-атаки за адресами пристроїв, перетворених на зброю, на кінець 2021 року (джерело: A10)

становив 10–20 хвилин, у 40% — менш ніж 10 хвилин. Водночас Cloudflare застерігає, що короткі атаки часто залишаються непоміченими, особливо якщо вони відбуваються у лічені секунди. У цьому випадку при ручному реагуванні зупинити атаку вчасно неможливо, залишається тільки провести аналіз і додати нові правила фільтрації трафіку.

Компанія ***Imperva***, зі свого боку, вважає, що тривалість атак скоротилася: понад 60% з них не перевищували 7 хвилин, і загалом майже 75% були коротшими за півгодини.

Що стосується жертв, то — повертаючись до Cloudflare — 8,2% байтів DDoS-трафіку були спрямовані проти компаній сфери телекомунікацій, 3,6% — проти індустрії азартних ігор, 3,3% — IT (якщо рахувати в пакетах, то відповідно 10,85%, 4,62% і 4%).

Вектори мережевих атак представлені на **рис. 2** — як видно, понад половини припадає на простий тип SYN flood. Водночас зростає кількість атак на базі протоколу SSDP, який використовується для підключення пристроїв типу «Plug and Play» (наприклад, мережевих принтерів) — за допомогою цього протоколу здійснюють атаки типу посилення/відображення, змушуючи пристрої завалювати мережу інформацією про себе.

Рис. 2. Вектори DDoS-атак мережевого рівня у 1 кварталі 2022 року (джерело: Cloudflare)

Imperva зазначає, що практично 80% атак були одновекторними. У майже 16% випадків використовувались одночасно 2 чи 3 вектори, і у 4% понад 4. Багатовекторні атаки стають менш чисельними, хоча постійно з'являються нові різновиди загроз.

Компанія A10, порахувавши IP-адреси знарядь атак (перетворених на кіберброю комп'ютерів, серверів, IP-камер та інших пристроїв), визначила, що зараз кількісно переважають атаки саме з використанням протоколу SSDP (**рис. 3**). За підрахунками компанії, у світі налічується 3 млн систем, що підтримують SSDP і є вразливими до атак. Ці пристрої, задіяні в атаках типу посилення і відображення, здатні генерувати трафік у 30 разів більший за розмір запиту.

Загалом впродовж 2021 року кількість пристроїв, перетворених на знаряддя DDoS-атак, у світі зросла на 161% і сягнула 15,4 млн.

Найбільшу кількість ботнет-агентів A10 нарахувала в Китаї (34% від загального числа), далі Індія (10%), США (6%), Мексика та Єгипет (по 5%).

Якщо вести мову про атаки прикладного рівня, то Cloudflare зазначає, що за минулі 12 місяців їх кількість значно зросла (на 164%): зокрема, протягом самого лише березня відбулось більше атак рівня HTTP, ніж за кожен з попередніх кварталів. При цьому, після чотирьох поспіль кварталів китайського домінування, на перше місце серед країн походження атак вийшли США, де їх число зросло на 6,78% порівняно з попереднім кварталом і на 2,23% за рік. Найбільше хакери атакували сектор споживчої електроніки.

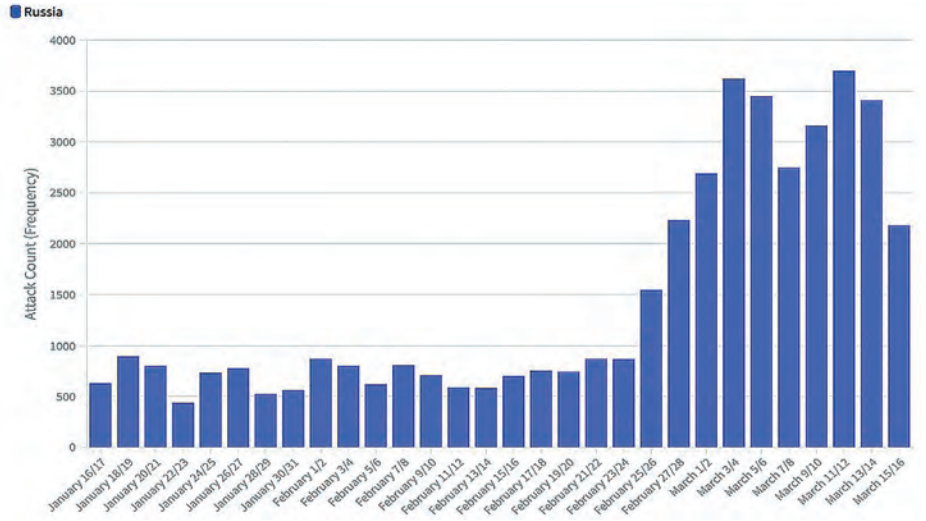


Рис. 4. Щоденна кількість DDoS-атак проти Росії у перші 2,5 місяця 2022 року (джерело: Netscout)

у «комерційних постачальників», що видно з їхньої тривалості: у третини вона не перевищувала 5 хвилин, загалом у 70% — 10 хвилин.

За даними Netscout, більшість атак була спрямована проти фінансового сектору Росії, далі з великим відривом слідують телерадіокомпанії та держустанови. (**рис. 4**)

Cloudflare у своєму звіті надає інший розподіл (чи то через відмінні дані, чи в силу того, що їхній матеріал свіжіший). Отже, на території Росії найчастіше зазнавали атак онлайн-медіа, Інтернет-індустрія, криптовалютні компанії й роздрібна торгівля. Більшість HTTP-атак здійснювалися з адрес Німеччини, США, Сінгапуру, Фінляндії, Індії, Нідерландів та України, хоча, зауважує компанія, визначення місця походження трафіку не рівнозначне атрибуції атакувальника. Що стосується України, то в нас головними цілями були теле- і радіомовники. Атаки здійснювались з більшого числа країн, що може свідчити про застосування глобальних ботнетів. Проте основна кількість походила з територій США, Росії, Німеччини, Китаю, Британії й Таїланду.

Анти-DDoS

Як і загалом у кіберзахисті, для боротьби з DDoS є різні стратегії. Функції анти-DDoS реалізовані в мережевих екранах. Існують апаратні системи, хмарні сервіси очистки трафіку, можна обрати й гібридний захист.

З ***апаратного боку***, наприклад, ***Radware*** пропонує системи для різного застосування: від невеликих корпоративних дата-центрів до телеком-операторів і провайдерів першого рівня. Ця лінійка, що має назву DefencePro, забезпечує захист як від атак великої потужності, так і від короткотривалих загроз. У ній, зокрема, реалізовані власні технології поведінкового аналізу та автоматизованої генерації сигнатур проти атак невідомого типу. Можливе розгортання як локально, так і в хмарі. У ***Netscout Arbor*** рішення Threat Mitigation System також працює апаратно, на віртуальних машинах або в хмарі (компанія має і власний сервіс захисту Arbor Cloud з глобальною здатністю очистки 11 Тбіт/с).

Є рішення анти-DDoS і у виробників систем комплексного захисту. Приміром, платформа ***Check Point*** DDoS Protector поєднує, власне, функцію анти-DDoS, мережевий поведінковий аналіз, систему протидії вторгненням і захист від атак через SSL. Платформа FortiDDoS від ***Fortinet*** має паралельну архітектуру, яка дозволяє автономно перевіряти трафік за понад 230 тис. параметрів — за твердженням виробника, рішення здатне виявляти атаку впродовж 2 секунд і інколи вже з першого пакета.

Хмарний анти-DDoS має загалом ті самі переваги, які взагалі притаманні SaaS– і подібним рішенням. Замовник платить за послугу відповідно до своїх потреб, при цьому він позбувається необхідності вибудовувати власну інфраструктуру кіберзахисту та тримати персонал відповідної кваліфікації. Постачальник послуги постійно оновлює базу відомих атак і чорні списки IP-адрес, за потреби модернізує апаратну частину. Окрім того, постачальник може мати виділений персонал, який слідкує за загрозами, вразливостями і аномаліями, що прискорює реагування. Оскільки ж постачальник обслуговує багатьох клієнтів, то за рахунок масштабу ціна знешкодження атаки, як правило, виходить для користувача нижчою ніж у випадку розгортання власних систем.

Сервіс анти-DDoS надають, зокрема, такі глобальні гравці, як ***Cloudflare***, ***Amazon*** (AWS Shield), ***Microsoft*** (у складі Azure), відносно новий провайдер Project Shield від ***Jigsaw*** — технологічного інкубатора ***Alphabet***, материнської компанії ***Google***. Як правило, послугу анти-DDoS пропонують телеком-оператори і місцеві провайдери на основі своїх мереж. Є цікаве рішення компанії ***Reblaze***, яка пропонує повністю хмарну платформу кіберзахисту, інтегровану з AWS, Google Cloud і Azire. Платформа використовує автоматизований процес навчання, що дозволяє виявляти атаки на ранніх стадіях.

Водночас хмарні рішення мають певні недоліки і обмеження. Зокрема, не всім компаніям може бути до вподоби вподоби віддавати свій трафік на очистку деінде; склад трафіку, що проходить мережами компаній, може різнитися, тоді як можливості постачальника підлаштуватися під потреби конкретного замовника не такі вже й великі. Оскільки очистка зазвичай працює не увесь час, а вмикається за потреби, це може спричиняти запізнілі реагування, тим більше що більшість атак, як вже зазначалося, тривають лічені хвилини. А у разі постійного включення пропуск трафіку через хмару спричинятиме зайві затримки.

Гібридний захист поєднує обидва варіанти: наприклад, очистку мережевого трафіку під час об'ємних атак можна віддати провайдеру, а локальна система захищатиме від атак прикладного рівня. Якщо ж апаратне рішення теж не справлятиметься, увесь трафік можна спрямувати до хмари. Так би мовити, найкраще з обох світів обов'язково вбереже.

Василь ТКАЧЕНКО, **МтБ**