Сучасний DDoS:

швидше, дошкульніше, потужніше

DDoS-атаки стають багатовекторними і б'ють по площах.

Мало того, що кількість DDoS-атак невпинно зростає з року в рік: самі вони стають дедалі складнішими і масштабнішими. Так російсько-українська кібервійна стала поштовхом для постання груп хактивістів, чиї мотиви вже й не пов'язані з нашими подіями, водночас більшає й традиційних атак з метою наживи. Хакери постійно шукають нових підходів, не гребуючи й старими; експерти відзначають збільшення тривалості атак і числа залучених пристроїв IoT, а також прогнозують поширення автоматизованих атак з використанням штучного інтелекту.

«МтБ» спробував розібратися в нинішніх трендах DDoS-атак. Дані про них є у відкритих джерелах, зокрема статтях та звітах вендорів. Ми також поцікавились у вітчизняних компаній — провайдерів та системних інтеграторів, які пропонують рішення та послуги захисту від DDoS — їхньою думкою щодо еволюції DDoS-атак і захисту від них.

Під ударом банки, IT й ігромани

Те, що DDoS-атак стає дедалі більше, навряд чи когось здивує. Компанії, які ведуть статистику, навіть не роками, а десятиліттями говорять про стабільне зростання кіберзлочинності. Але DDoS-атаки можна оцінити за кількісними показниками об'єму трафіку, задіяного в цих атаках. Вони також зростають.

Так, у 2021 році ***Microsoft*** зупинила найбільшу на той момент DDoS-атаку, спрямовану на одного з користувачів Azure, вона мала рекордні значення швидкості у 3,45 Тбіт/с і 340 млн пакетів на секунду.

В серпні 2023 року ***Google*** зупинила серію атак, які на піку сягали 398 млн запитів на секунду. Вони були спрямовані проти сервісів Google і хмарної платформи Google Cloud. У цих атаках було застосовано новий метод

ХАКЕРИ ПОВЕРНУЛИСЬ ДО АТАК РІВНІВ L3/L4

До DDoS-атак у світі сьогодні доєднався український сегмент. Це можна пояснити двома фактами. По-перше, атаки відбуваються через точку обміну трафіком UA-IX, де присутній не тільки наш трафік, але й зарубіжний. І, наскільки б дивно не звучало, складові IoT-мережі стають частиною ботмереж та відповідно й атак. Банально це наші холодильники, зубні щітки. Втім, сьогодні їхній вплив у загальній кількості атак мізерний.

Тривають і кібератаки на українську інфраструктуру. Якщо у 2021 році їх кількість становила 1400, то у 2022-му і 2023-му цифра перевищила позначку 4500. І мова наразі йде лише про потужні кібератаки, які фіксує і відбиває саме СБУ. Хоча за останні місяці їх стало дещо менше, вони стали не такими хаотичними і більш таргетованими. Тепер кожна атака має під собою конкретну ціль.

Минулого року хакери здебільшого використовували «інтелектуальні» атаки рівня L7, направлені на пошук слабких місць в інфраструктурі. Цього року вони повернулися до атак рівня L3 та L4. Причиною тому є специфіка атак рівня L7. Проаналізувавши таку атаку, кіберфахівці компанії напишуть правило, яке унеможливить її в майбутньому. З атаками рівня L3 та L4 складніше. Адже вони є лавинними, і написати одне-два правила, аби захиститися від них, неможливо.

З іншого боку, DDoS-атаки з ознаками L3 та L4 рівня насправді сьогодні відносяться до L7. Це пояснюється великою кількістю запитів з різної кількості IP-адрес до сервера, причому коректних запитів нібито від потенційних клієнтів. Раніше така тенденція не спостерігалася.

Назарій КУРОЧКО,
засновник групи компаній GIGAGROUP та телеком-оператора GigaTrans

під назвою HTTP2/Rapid Request, який експлуатує особливість протоколу HTTP2, а саме підтримку одночасно багатьох (до 100) потоків даних HTTP в сесії TCP. Отже, метод полягає в тому, що клієнт ініціює велику кількість потоків і негайно надсилає запити на скасування. Так сервер перевантажується обробкою завдань, а атакуюча сторона не перевищує граничної кількості одночасних потоків.

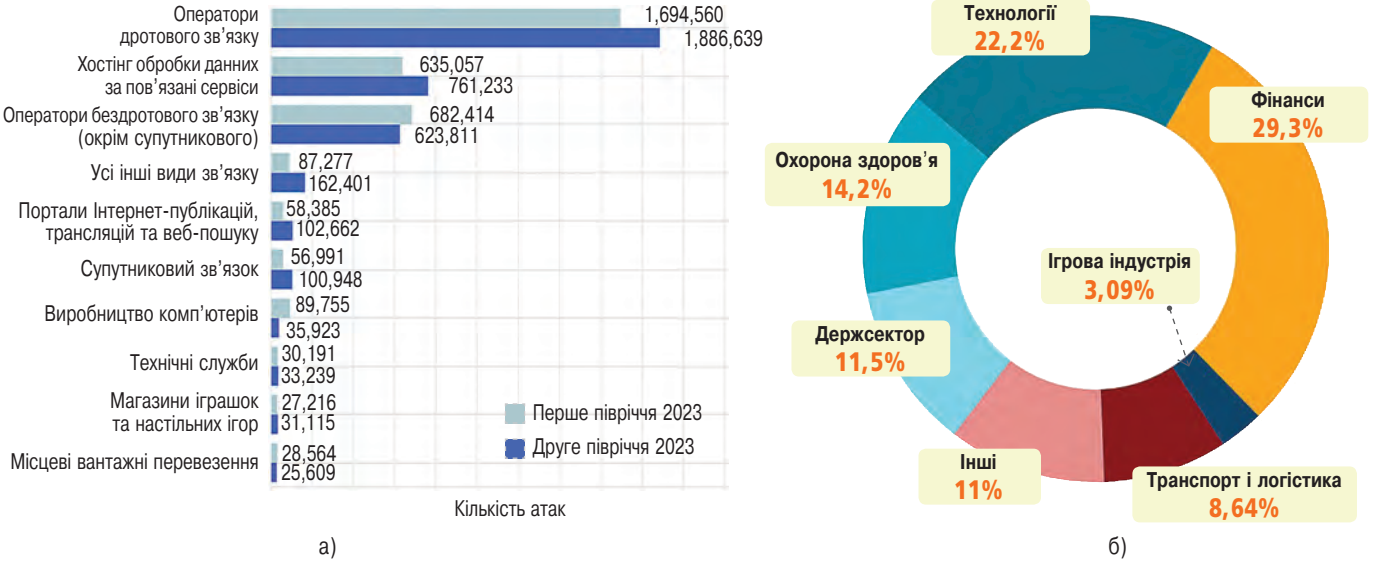
Компанія ***Cloudflare*** у 4 кварталі минулого року також відзвітувала про відбиття потужної атаки такого самого типу у 201 млн запитів на секунду.

Cloudflare зафіксувала впродовж 2023 року понад 5,2 млн DDoS-атак рівня HTTP, що разом склало понад 26 трлн запитів. Проте, як не дивно, кількість цих атак виявилась на 20% меншою, ніж у 2022-му. Водночас на мережевому рівні спостерігався протилежний тренд: автоматизований захист відбив 8,7 млн атак, тобто на 85% більше, ніж у році попередньому. З-поміж усіх атак 91% тривали менш ніж 10 хвилин, лише 2% — понад годину; 97% на піку генерували менш ніж 500 Мбіт/с, і 88% не перевищували 50 тис. пакетів на секунду.

Radware у звіті 2024 Global Threat Analysis Report подає такі цифри: середня кількість DDoS-атак, що їх блокували компанії-клієнти, зросла на 94% проти 2022 року. При цьому середній об'єм атаки зріс на 48%. На 63% збільшилась кількість невеликих атак (до 1 Гбіт/с), тоді як атак від 100 до 250 Гбіт/с стало на 177% більше, а понад 500 Гбіт/с — на 150%.

Netscout у своєму звіті DDoS Threat Intelligence Report зазначає, що у другому півріччі минулого року нею було зафіксовано понад 7 млн DDoS-атак — на 15% більше, ніж у першому (загалом у 2023 році компанія спостерігала понад 13 млн DDoS-атак). З них найбільше — понад 3,5 млн, або 53% від загального числа — тривали від 5 до 15 хвилин. За об'ємом найпоширенішими (35%) були атаки від 100 Мбіт/с до 10 Гбіт/с.

За даними Netscout, цілями атак є здебільшого компанії зі сфери IT і телекомунікацій (**рис. 1 а**). Radware (**рис. 1 б**)



а) б)

Рис. 1. Топ цілей DDoS-атак у 2023 році за сферами індустрії. Дані Netscout (а) і Radware (б)

ЧЕРЕЗ ХМАРНІ РЕСУРСИ ЗАПУСКАЮТЬ МАСОВАНІ DDOS-АТАКИ

За нашими оцінками, динаміка DDoS-атак в Україні значно змінилася порівняно з першим роком вторгнення. Їх кількість продовжує зростати, зокрема з'являється все більше сервісів з найму для DDoS-атак, що дозволяє кіберзлочинцям легко організовувати великі атаки з мінімальними витратами. Типи атак також еволюціонували, ставши більш складними та різноманітними. В обсязі середній розмір атак зріс до кількох терабіт на секунду, що ставить під загрозу навіть великі Інтернет-ресурси. Основними цілями DDoS-атак залишаються критична інфраструктура, урядові та комерційні організації, але збільшилася частка атак на платформи, пов'язані з онлайн-сервісами та фінансовими операціями. Це свідчить про те, що кіберзлочинці використовують DDoS як інструмент для дестабілізації економіки та створення паніки серед населення.

Цікаво, що у 2023 році значно збільшилась кількість DDoS-атак, для запуску яких зловмисники активно використовували ресурси хмарних обчислень, такі як віртуальні машини. Наприклад, скомпрометовані підписки Azure використовувалися для генерації ресурсів у 40 регіонах щомісяця, що демонструє глобальне охоплення шкідливих ботнетів. Завдяки цьому зловмисники можуть запускати атаки з величезними обсягами трафіку, що потребує значних зусиль для їх нейтралізації. За даними Microsoft, в кінці року спостерігалися атаки з піковими значеннями до 90 Тбіт/с. По-друге, помітно змінився основний вектор атак: домінуючим став TCP, тоді як раніше переважали UDP-атаки. Це зміщення пов'язане з активізацією діяльності хактивістських груп та збільшенням використання сервісів DDoS на замовлення.

Андрій ЛЕВЧЕНКО,
бренд-менеджер A10 Networks в ilT Distribution

У найближчому майбутньому можемо очікувати зростання ролі розподіленого захисту, який здатний виявляти та нейтралізувати атаки в реальному часі і навіть на великих швидкостях обміну даними (деякі розробники WAF вже активно впроваджують системи ботменеджменту і т.д.). Окрім цього, прогнозуємо збільшення використання штучного інтелекту та машинного навчання для аналізу трафіку та виявлення аномалій, що допоможе вчасно реагувати на нові види атак. Зараз дуже багато WAF-ів працюють на основі регулярних виразів (regex) або на прописаних логічно правилах. Кількість автоматизації та залучення ШІ для зменшення помилкових спрацювань буде збільшуватись в рази.

наводить іншу статистику: майже 30% усіх атак припадає на фінансовий сектор, трохи більше ніж 22% — на технологічні компанії. При цьому підприємства зі сфери транспорту й логістики зазнали на 36% більше атак, ніж у 2022 році, комунальні служби — на 23% більше, а телекомунікаційні компанії і провайдери послуг — навпаки, менше (але не набагато: відповідно на 0,5% і 0,6%). Згідно ж із даними Cloudflare за 4-й квартал, на прикладному рівні найбільше атак зазнавали сфера криптовалют, ігрова індустрія і азартні ігри, а також телекомунікації. На мережевому 45% DDoS-трафіку було спрямовано на сферу IT та Інтернету.

Netscout називає сферою, де DDoS-атаки чинять найбільший вплив, ігрову індустрію та пов'язані з нею азартні ігри. Мотивів для атак два: гроші, які крутяться в цій галузі, і бажання нашкодити конкурентам. Ігрова індустрія сильно залежить від цифрової інфраструктури і є дуже медійною. Атаки часто відбуваються під час геймерських турнірів. Вони не лише погіршують якість гри, а й становлять загрозу для стабільності роботи геймінгових платформ. В одному з прикладів певний геймінговий провайдер зазнав багатофазової атаки, яка порушила роботу не лише ігрових, а й критичних операційних сервісів, після чого відбулись інші кібератаки, кульмінацією яких стало викрадення даних з вимаганням викупу.

На іншу компанію, що оперує платформою, за допомогою якої користувачі можуть самі створювати ігри, було вчинено DDoS-атаки, об'єм яких був удесятеро більший за середній по індустрії, причому в них брали участь самі користувачі заради конкурентної переваги над суперниками. Дослідники знайшли в Інтернеті безліч інструментів, за допомогою яких геймери можуть ідентифікувати суперників і запускати проти них прості DDoS-атаки.

DDoS як продовження політики іншими методами

Однією з найбільш значних змін у ландшафті DDoS за останні роки є діяльність груп хактивістів, які, за формулюванням Netscout, «бомбардують веб-сайти й організації по всьому світу». Зокрема найактивнішим було угрупування Noname057(16), яке у другій половині минулого року атакувало 780 веб-сайтів у 35 країнах. Ця прокремлівська організація, яка вийшла на арену на початку 2022 року, має своє власне програмне забезпечення, атакує країни НАТО і використовує «гейміфікацію» кібервійни: пропонує винагороди у цифровій валюті за участь у кібератаках. Ця стратегія не лише збільшує масштаб операцій, але й «демонструє унікальний спосіб мобілізувати підтримку у цифровій сфері». Також угрупування використовує децентралізовані ботнети і публічні хмарні та хостингові сервіси, що суттєво зменшує кошти й ризики.

Інше угрупування, Anonymous Sudan, на деякий час затьмарило навіть Anonymous057(16), ця флуктуація підкреслює постійну мінливість ландшафту кібератак, зазначається у звіті Netscout. Угрупування зокрема відзначилось атаками проти месседжингових платформ X (колишній Twitter) і Telegram: у першому випадку — щоб спонукати Ілона Маска запустити сервіс Starlink у Судані, а у другому — аби помститися за закриття їхнього основного каналу. Anonymous Sudan пов'язане з російським угрупуванням Killnet, загалом має проросійські нахили і атакує, зокрема, стрімінгові платформи в пікові години.

На **рис. 2** показана статистика DDoS-атак проти російських та українських цілей за даними Netscout. Компанія зауважує, що наплив атак різних хактивістів викликаний також більш недавніми конфліктами, такими як ізраїльсько-палестинський, тож кількість атак щодня у другій половині 2023 року

АТАКИ СТАЮТЬ БІЛЬШ СКЛАДНИМИ І МАСШТАБНИМИ

З початку повномасштабного вторгнення ми бачимо постійне зростання кількості кібератак. Перші роки це були переважно атаки з використанням ботнетів, основною метою яких було паралізувати ключові інфраструктурні об'єкти та урядові веб-сайти, медіаресурси. З часом, після зміцнення заходів захисту, методи атак також стали більш складними – ворог почав використовувати багатовекторні DDoS-атаки, які важче виявити та блокувати.

Якщо казати про об'єкти DDoS-атак в Україні, то це державний сектор, фінансові установи, медіа, IT-сектор та логістика.

Що до еволюції DDoS-атаки можна виділити деякі напрями: збільшення їх масштабу; використання розподілених ботнетів; використання багатовекторних атак. Окрім того, зловмисники постійно шукають нові вразливості в мережевих протоколах та програмному забезпеченні для використання їх у DDoS-атаках.

Розвиток технологій захисту відбувається відповідно до розвитку характеру самих DDoS-загроз та з урахуванням останніх технологічних тенденцій. Одним з основних напрямків, які можуть покращити ефективність захисту від DDoS-атак, є застосування штучного інтелекту (ШІ) та машинного навчання розпізнавання й фільтрації зловмисного трафіку. Використання хмарних сервісів може дозволити компаніям та організаціям захищати мережу від DDoS-атак без необхідності утримувати власне обладнання та інфраструктуру. Такі хмарні сервіси надають розподілений захист та масштабування для ефективної фільтрації трафіку.

Микола МОЙСАК,
керівник відділу продажів
та розвитку бізнесу NWU

Деякі захисні системи можуть аналізувати поведінку користувачів для виявлення підозрілої активності, яка може бути пов'язана з DDoS-атаками. Наприклад, аналіз невиправданого збільшення запитів до сервера може виявити спроби DDoS-атак.

збільшилась удесятеро порівняно з першою половиною. Головними цілями були інфраструктура зв'язку, лікарні та банки.

Російські хакерські угрупування часто називають свої дії «покаранням» за допомогу Україні, але вони також не цураються використовувати як виправдання місцеві приводи. Наприклад, коли Noname057(16) запустили низку атак проти іспанських веб-сайтів, вони не лише послалися на підтримку України іспанським урядом, але й заявили про власну підтримку місцевих пожежників, які вимагали покращення соціального захисту. Атаки і протести відбувались на тлі виборів, що свідчить про бажання хакерів також «долучитися» до процесу.

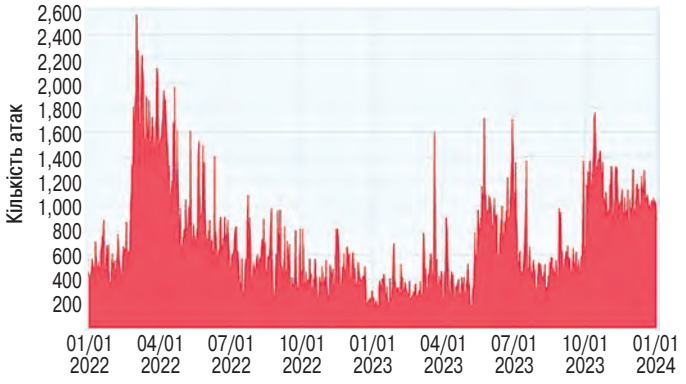


Рис. 2. Сукупна кількість DDoS-атак проти росії та України у 2022–2023 рр. (джерело: Netscout)

Загалом ескалація DDoS-атак характерна для періодів значних політичних потрясінь, пише Netscout. Наприклад, у грудні 2023 року в Перу їхня кількість зросла на 30% і то після подвоєння у році попередньому. Цей сплеск відбувся на тлі загальнонаціональних протестів, які збіглися з виходом з в'язниці колишнього президента Альберто Фухіморі. Ближче до нас, у Польщі, наприкінці року кількість атак зросла майже вчетверо порівняно з середнім для країни: саме тоді там відбувалися вибори, на яких змінилась правляча сила. Тоді ж було зроблено низку заяв про подальшу підтримку України, що спричинило «ідеальний шторм» для противників цієї позиції.

В Cloudflare порахували, що у 4 кварталі минулого року трафік DDoS, спрямований проти Тайваню, підскочив на 3370% порівняно з аналогічним періодом минулого року — це відбувалося на тлі виборів і напруги у відносинах з Китаєм. DDoS-трафік, спрямований на ізраїльські сайти, збільшився на 27%, а на палестинські — на 1126%, і загалом 10% всіх HTTP-запитів на палестинські веб-сайти (1,3 млрд) були DDoS-атаками, з них 90% були спрямовані проти сайтів банків. На мережевому рівні проти палестинських мереж було спрямовано 479 ТБ трафіку — 68% загалом, що зробило палестинські території другим (після Китаю) найбільш атакованим регіоном на планеті. Для порівняння, проти Ізраїлю запустили 2,4 ТБ трафіку.

З іншого боку, Radware, виходячи зі статистики оголошень про атаки в Telegram-каналах, називає найбільш атакованою країною саме Ізраїль (1450 атак), на другому місці Індія (1242), на третьому США (1164). Україна посідає 4-те місце (731), і разом з нами постраждала Польща (580).

Повертаючись до даних Cloudflare: на приголомшливі 61839% зріс DDoS-трафік проти веб-сайтів служб захисту довкілля під час конференції ООН зі зміни клімату (COP28). У 4 кварталі він склав половину усього трафіку DDoS-атак рівня HTTP. Згідно з архівними даними, попереднім конференціям (COP27 і COP26) також передували помітні сплески атак на сайти організацій з охорони довкілля.

Radware, проводячи моніторинг хакерських Telegram-каналів, ще відзначає такий факт: у 2023 році значно зросла кількість сервісів DDoS в найм. Чимала частина їх — російськомовні. Одне з потенційних пояснень полягає в тому, що хактивісти набули досвіду, і водночас їм набридло працювати на спільноту, коли можна зайнятись більш прибутковою справою — здавати напрокат свої інструменти і бот-мережі.

НЕОБХІДНО ПОСТІЙНО ВДОСКОНАЛЮВАТИ ЗАСОБИ КІБЕРЗАХИСТУ

Опираючись на показники незалежних досліджень та реальні атаки на наших клієнтів, можна з впевненістю сказати, що динаміка DoS/DDoS-атак збільшилася в порівнянні з 2022 роком, оскільки зросли об'єми бот-мереж та кількість аматорських атак. Оскільки засоби для проведення DoS/DDoS-атак знаходяться в загальному доступі, будь-хто має можливість скористатися даним програмним забезпеченням. Проте цілі атак за останні 2 роки не змінилися.

Враховуючи те, що прямий доступ з боку країни-агресора та її союзників – закритий, збільшилися випадки використання зловмисниками VPS/VDS-серверів в ЄС чи США шляхом використання ресурсів відомих хмарних провайдерів, а також використання різноманітних безкоштовних VPN– чи Proxy-мереж.

Майже після кожної DoS/DDoS-атаки зловмисники адаптуються та удосконалюють власні засоби атак, через що виникає необхідність постійного удосконалення засобів захисту публічних ресурсів на стороні компаній. Удосконалення засобів захисту полягатиме в першу чергу у модифікації підходів виявлення DoS/DDoS-атак, і пов'язано це з тим, що Україна зараз знаходиться в стані війни не тільки на фронті, але і в кіберпросторі, де від останнього залежить функціонування інформаційних засобів в межах держави, працездатність економічного сектору, працездатність критичних сервісів країни тощо.

Євгеній ПЕДЧЕНКО,
керівник відділу систем інформаційної безпеки ТОВ «СІТОН-ГРУП»

Тренди: DNS, хмари, штучний інтелект

Компанія ***Akamai*** у своїх звітах фіксує зростання кількості «горизонтальних DDoS-атак», або ж атак типу «килимове бомбардування». На відміну від «вертикальних», які спрямовані проти однієї вагомої цілі (як-от веб-сайт організації), горизонтальні здійснюються одночасно проти багатьох. Наприклад, хакери можуть спробувати «покласти» усі IP-адреси, які належать організації, або атакувати одночасно різні сервіси та системи. Akamai пише, що до третього кварталу 2022 року менше 20% DDoS-атак, які вона спостерігала, можна було віднести до горизонтальних, але відтоді і до 3 кварталу 2023-го таких було вже 30%.

Ще дослідники відзначають зростання числа векторів, які злочинці використовують одночасно. Цитуючи знову-таки Akamai, деякі з-поміж наймасштабніших і найскладніших атак, які фіксувались цією компанією, включали 14 або й більше різних векторів і явно мали на меті виснаження можливостей груп кіберзахисту. У багатьох випадках такі комплексні багатовекторні DDoS-атаки служили прикриттям у кампаніях потрійного здирництва.

Важливим трендом, який згадують усі дослідники, є атаки проти DNS-серверів. Netscout пише, що зловмисники вже не задовольняються виведенням з ладу одного веб-сайту або сервера, а натомість прагнуть покласти системи, блокування яких завдасть великих супутніх збитків. DDoS-атаки можуть порушувати роботу багатьох доменів, які використовують одну й ту саму веб-інфраструктуру, що є або ненавмисним побічним ефектом, або входить у плани хакерів як спосіб приховати справжню ціль. Розслідування показало, що в середньому атака проти одного домену зачіпає сім інших. У 15% атак страждали від 100 до 100 тис. веб-сайтів.

Оскільки авторитетних серверів (тобто тих, які власне зберігають IP-адреси) відносно небагато, успішні атаки проти них завдають надзвичайно великої шкоди. За підрахунками Netscout, атаки типу DNS query flood, розраховані проти авторитетних DNS-серверів, у другому півріччі минулого року зросли на 553% порівняно з першим, і загалом компанія спостерігає 50–100 таких атак проти DNS-інфраструктури щодня. Не рідкістю є й потужні атаки у мільйони запитів на секунду.

Хакери користуються старіючим парком IoT-пристроїв, а також слабкими і дефолтними паролями у підключених до публічних мереж пристроях і серверах, пише Radware. Приватні IoT-пристрої є ідеальною базою для вчинення атак з використанням псевдовипадкових субдоменів (PRSD), також відомих як «катування питтям» (DNS Water Torture), тобто коли ці пристрої використовують DNS-резолвери для атак на авторитетні сервери.

Окрім того, йдеться у звіті Radware, відбувається міграція хакерів у хмари. Вони змінюють скомпрометовані IoT-пристрої на набагато вигідніші за показником «кошти/ефективність» хмарні сервіси, де можуть облаштовувати потужні вузли. Відповідно хакери мають цілковитий контроль над своїми серверами, можуть не боятися випадіння пристроїв через перезавантаження, а також менше наражаються на ризик викриття.

Але чинником, на який Radware звертає увагу насамперед, є поява великих мовних моделей (LMM), які не обмежені природними мовами і добре надаються до програмування. Не надто вмілі хакери використовують LLM для написання складніших скриптів або зловмисного коду, проте, оскільки цей код обмежений знаннями, на яких натреновано LLM, в сукупності зростає не складність самих атак, а кількість атак більшої складності. Хакери використовують LLM для пришвидшення запуску атак, і навіть для досвідчених злочинців цей інструмент відкриває нові можливості, такі як автоматизація пошуку вразливостей.

З іншого боку, штучний інтелект використовується і для боротьби з DDoS-атаками. Виробники вже давно втілюють інструменти ШІ та машинного навчання для виявлення аномалій в мережевому трафіку, підозрілої поведінки користувачів, прогнозування DDoS-атак та автоматизації протидії. Колись у майбутньому цю кібервійну вестимуть роботи.

Василь ТКАЧЕНКО, МтБ