DDoS-атаки: більше не прихована загроза у світі Інтернету

Щоб убезпечити ресурси і застосунки, потрібен ешелонований захист.

Сьогодні багато кіберзлочинів вже можна замовити онлайн через численні сайти, що є у відкритому доступі. Будь-яка людина, яка має вихід в Інтернет, може купити атаку на бажаний онлайн-ресурс, до того ж зробити це не складніше, ніж замовити доставку піци.

DDoS-атака — купити!

«Найкраще розв'язання Ваших проблем. Швидко. Якісно. Низькі ціни». Звучить як реклама салону краси або шиномонтажу (**рис. 1**).

Деякі «клієнтоорієнтовані» зловмисники навіть пропонують «пробні» атаки на 10 хвилин, щоб показати ефективність своїх інструментів.

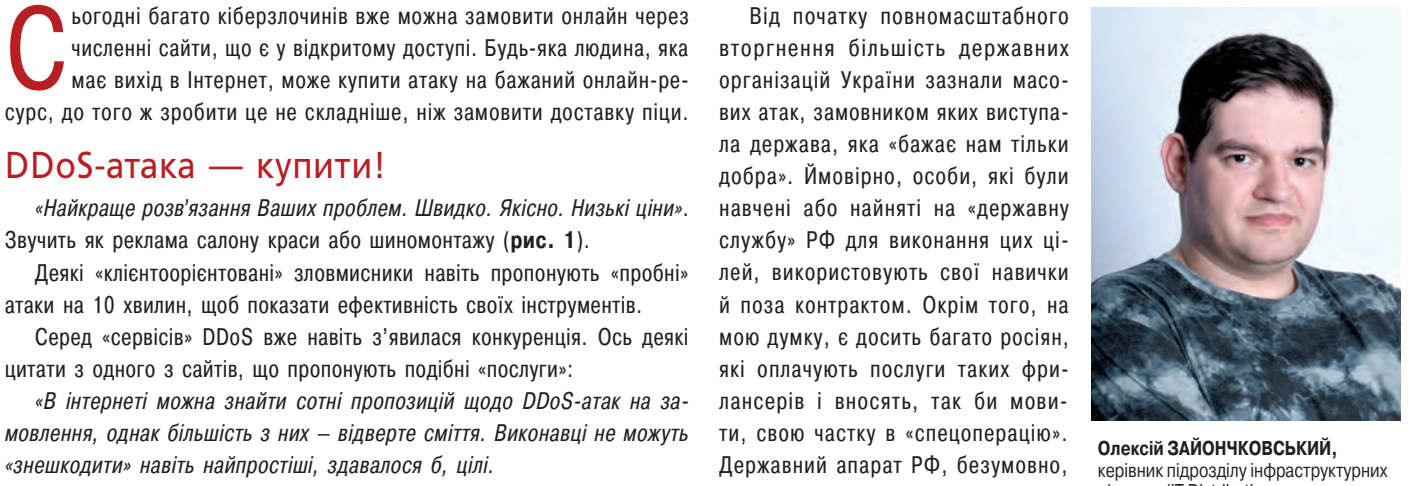
Серед «сервісів» DDoS вже навіть з'явилася конкуренція. Ось деякі цитати з одного з сайтів, що пропонують подібні «послуги»:

«В інтернеті можна знайти сотні пропозицій щодо DDoS-атак на замовлення, однак більшість з них – відверте сміття. Виконавці не можуть «знешкодити» навіть найпростіші, здавалося б, цілі.

Ми займаємося DDoS-атаками вже понад три роки і є професійною та висококласною командою, яка НЕ буде вас ігнорувати, загинати ціни, давати неправдиві обіцянки й надії».

Розцінки на знімку екрана (**рис. 2**).

Усе це свідчить лише про одне: тіньовий світ вийшов з підпілля і пропонує свої послуги з «ліквідації» конкурентів відкрито і за досить низьку вартість. Багато подібних сайтів використовують міжнародні домени, але чомусь можуть приймати оплату в рублях РФ. Дивний збіг, чи не так?



Від початку повномасштабного вторгнення більшість державних організацій України зазнали масових атак, замовником яких виступала держава, яка «бажає нам тільки добра». Ймовірно, особи, які були навчені або найняті на «державну службу» РФ для виконання цих цілей, використовують свої навички й поза контрактом. Окрім того, на мою думку, є досить багато росіян, які оплачують послуги таких фрилансерів і вносять, так би мовити, свою частку в «спецоперацію». Державний апарат РФ, безумовно, не проти атак як на українські, так і на західні компанії, тому не буде займатися пошуком та притягати до відповідальності зловмисників, які відверто вчиняють злочини в кіберпросторі.

Крім «професіоналів-найманців», є також «добровольці», які влаштовують цілеспрямовані атаки на українські ресурси. У наведеній нижче спільноті перебуває близько 30 000 осіб, які регулярно атакують українські приватні компанії та державні організації (**рис. 3**).

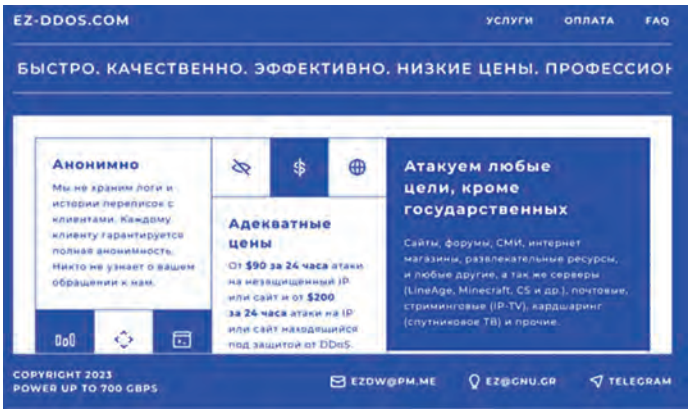


Рис. 1. Так виглядає типова реклама DDoS-атаки на замовлення

Рис. 2. «Прейскурант» зловмисників. Не так і дорого

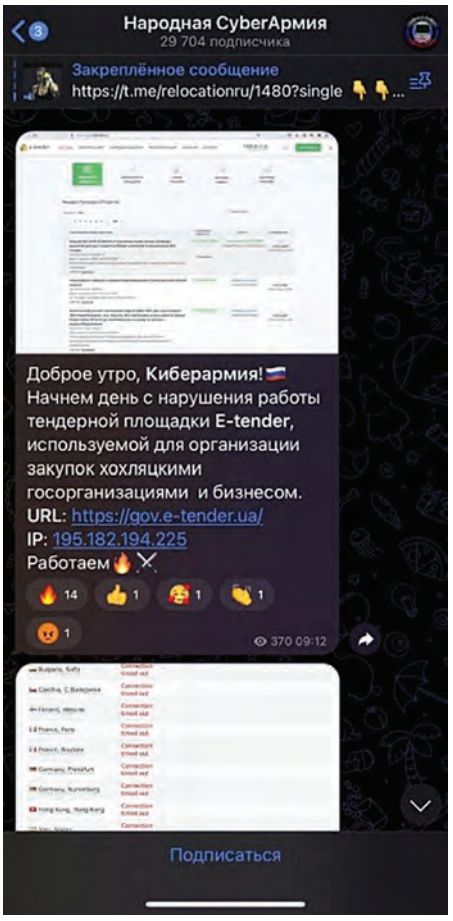


Рис. 3. «Народна кіберармія». Росіяни вкрали й цю ідею, залучивши хакерів-добровольців

Хто під прицілом?

Під монолітні DDoS-атаки, тобто атаки, метою яких є саме припинення роботи деяких ресурсів, зазвичай підпадає середній бізнес. У розпорядженні таких компаній є досить цінні сервіси, відмова яких може спричинити негативні фінансові наслідки, проте вони не мають достатньо коштів та компетенції для забезпечення ефективного захисту від DDoS-атак та кіберзагроз загалом. Часто власники такого бізнесу не усвідомлюють ризиків або не вірять, що ці ризики можуть мати наслідки, доки не стикаються з повідомленням про недоступність їхнього вебсайту.

Великі бізнеси зазвичай стають жертвами DDoS-атак не стільки з метою припинення доступності їхніх систем, скільки для прикриття інших кіберзлочинів. У більшості сучасних спланованих DDoS-атак використовують множинні вектори, тобто одночасно кілька механізмів для придушення цільового об'єкта. Це може включати перевантаження мережевих пристроїв по маршруту, спроби «забити» канали комунікації, атаки на DNS, а також безпосереднє зловживання ресурсами серверів та застосунків. Захист від такого комплексу атак істотно складніший, і далеко не завжди ці атаки можна виявити на рівні провайдера. Якщо атаки об'ємами пакетів досить легко виявляються і можуть бути ліквідовані Інтернет-провайдером, то спеціалізовані L7-атаки на сервери застосунків та веб-сервіси не потребують великих обсягів трафіку, і провайдер може легко їх пропустити, оскільки надає пріоритет захисту каналів і не розуміється на тому, як мають працювати сервіси компанії-клієнта.

DDoS-атаки часто є «гучним» прикриттям для інших зловмисних дій. У той час як команда SOC отримує величезну кількість сповіщень від усіх систем, дуже складно зрозуміти істинний задум зловмисника і які сервіси насправді є метою.

Трохи цифр

Згідно з нещодавнім звітом про DDoS-загрози за 2022 рік від лідера ринку рішень для балансування трафіку та захисту периметра мереж – компанії **A10 Networks** – у світі зафіксовано понад 15 мільйонів одиниць DDoS-зброї, причому кількість нетипового інструментарію зросла вдвічі порівняно з минулим роком. З 2019 року по 2021-й цей показник збільшився на 161%, включно з «відбивачами» трафіку і ботнетами. Таке зростання з високою ймовірністю триватиме далі, оскільки світ активно насичується IoT-пристроями. Щосекунди до глобальної мережі під'єднується 127 нових пристроїв – це різноманітні датчики, розумні домашні гаджети, персональні маршрутизатори, телевізори, ігрові консолі, камери відеоспостереження тощо. Проблема цих пристроїв в тому, що їхнє ПЗ практично ніколи не оновлюється, а отже, вони є вразливими до атак вірусів, які перетворюють їх на «зомбі» та під'єднують до центрів віддаленого управління.

Оскільки лідером виробництва всілякого роду ґаджетів є Китай, то очевидно, що ця країна є лідером і за кількістю DDoS-зброї, маючи у своєму розпорядженні понад два мільйони інструментів (34% світового обсягу). У 2021 році було виявлено понад 423 000 бот-мереж, які ґрунтувалися на заражених IoT-пристроях.

Основними протоколами, які використовуються для DDoS, залишаються SSDP, PortMap, SNMP, DNS, TFTP.

Природа UDP-протоколів, які для прискорення роботи не перевіряють джерело оригінального запиту, дає змогу посилювати та множинно відбивати запити. Зловмисник спочатку маскується під жертву атаки та відправляє велику кількість невеликих запитів, відповіді на які доставляються вже реальній жертві. Аналогією може бути дзвінок у піцерію з підробленої сім-карти і замовлення сотні піц на адресу жертви з терміновою доставкою без додаткового дзвінка і оплатою кур'єру...

Використання SSDP – а в Інтернеті зараз понад 3 000 000 пристроїв, які радо надають інформацію за цим протоколом, – може посилити атаку в 30 разів! Таким чином, наприклад, було реалізовано атаку на AWS з пропускною спроможністю у 2,3 Терабіта!

Ешелонований захист

Всупереч розхожій думці, що наземні системи DDoS захисту – це рудимент, є певна кількість сценаріїв, за яких це єдина опція для вибору:

1. **Затримки.** Перенаправлення трафіку в хмару вносить додаткові затримки, які не завжди задовольняють вимоги застосунків і якості сервісу.

2. **Рівень контролю налаштувань.** Хмарні сервіси можуть надавати адекватний захист для типових сервісів, але не мають гнучких можливостей налаштування та не здатні якісно захистити спеціалізовані застосунки. Наприклад, більшість великих ігрових компаній захищають свої сервери наземними рішеннями, оскільки їхня специфіка потребує значної кастомізації.

3. **Внутрішні стандарти та вимоги регуляторів.** Не всі компанії можуть перенаправляти трафік в інші країни для аналізу та очищення. Під такі вимоги часто потрапляють державні організації та інші сектори, залежно від регіону.

4. **Рівень довіри та залежність.** Хоча частка хмарних сервісів неухильно зростає, існує достатня кількість великих організацій, які не довіряють управління навіть частиною своєї інформаційної безпеки хмарним провайдерам послуг.

Оптимальним, як і у випадку мережевих екранів, є ешелонований або гібридний захист. Він передбачає, що інтернет-провайдер забезпечуватиме захист від грубих об'ємних атак, тоді як локальні системи протидіятимуть перевантаженню серверного обладнання та відповідних сервісів. У такому випадку можна також залучати хмарного провайдера для очищення загального трафіку, а захист специфічних застосунків, які може «покласти» невелика кількість трафіку, забезпечити локально.

На додачу наземні системи захисту від DDoS можуть забезпечувати додаткові функції. Наприклад, обладнання компанії ***A10 Networks*** може виступати додатково як:

- балансувальник навантаження (ADC) для On-Premise і гібридних інфраструктур;
- шифратор/дешифратор SSL для розвантаження інших пристроїв безпеки;
- веб-екран на базі рішення від Fastly;
- екран для захисту DNS.

Враховуючи відсутність окремих ліцензій на кожну частину функціональності, комплексне рішення є досить недорогим і, порівняно з конкурентами, не поступається ні в продуктивності, ні в технологічності.

З огляду на поточну ситуацію, коли DDoS-атаку можна замовити за п'ять кліків, актуальність та необхідність впровадження відповідних рішень для захисту від DDoS продовжуватиме зростати не тільки для великих компаній, а й для організацій середнього розміру, які також перебувають під постійним прицілом.

Консультацію та підбір рішень для ефективної протидії DDoS здійснюють експерти компанії iIT Distribution. Для отримання детальної інформації звертайтеся за контактами: +38(044)339 91 16; a10@iitd.io
Офіційний сайт: www.iitd.com.ua