СП «Інфоком»
вул. Володимирська, 8
Київ, 01001, Україна
тел.: +380 (44) 230 52 00
infocom@infocom.ua
infocom.ua

infoDDoS

Захист від DoS/DDoS-атак

infocom.ua

2024

ІНФОРМАЦІЙНА БЕЗПЕКА

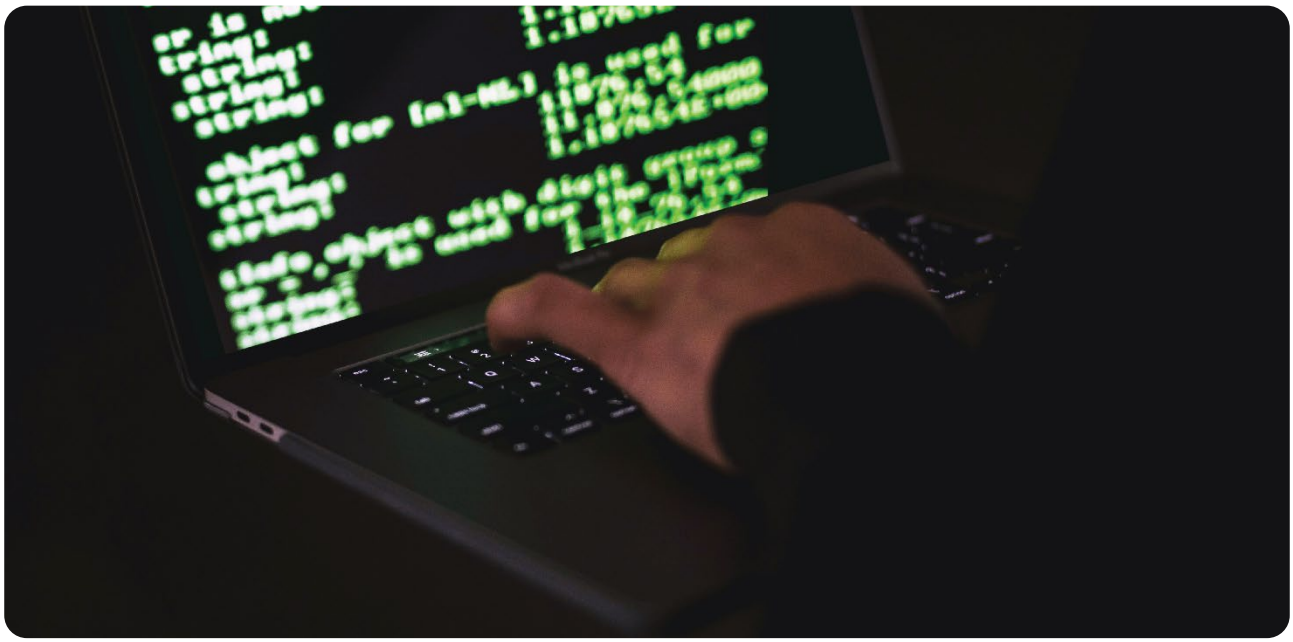
Робота державної чи фінансової установи, великого або малого бізнесу, навчального чи медичного закладу нерозривно зв'язана з використанням цифрових інформаційних технологій, які, в значній мірі, дозволяють спростити, впорядкувати, автоматизувати та значно підвищити ефективність усіх наявних організаційних, фінансових, виробничих або будь-яких інших процесів. Будь-яке несанкціоноване втручання у роботу відповідної інформаційної інфраструктури збоку зловмисників або недоброчесних конкурентів може не тільки тимчасово зупинити важливі робочі процеси але й через виток конфіденційної внутрішньої інформації призвести до значних репутаційних або фінансових втрат.
Послуги Infocom з інформаційної безпеки покликані мінімізувати будь-які ризики несанкціонованого доступу у вашу інформаційну інфраструктуру та забезпечити її надійне та безперервне функціонування завдяки всебічному захисту як зовнішнього так і внутрішнього периметру.

infoDDoS

web-сторінка послуги

БЕЗПЕРЕРВНА РОБОТА РЕСУРСІВ ЗАВДЯКИ ЗАХИСТУ ВІД DOS/DDOS АТАК

У сучасному світі веб-портал є важливим інструментом ведення бізнесу, зупинка якого може призвести до недоотриманого прибутку, репутаційних та прямих фінансових втрат. Це особливо характерно для інтернет-торгівлі, банків, платіжних систем та усіх інших, чия робота глибоко пов'язана, або повністю залежить від взаємодії з клієнтом через власний веб-портал. Зловмисники знають про важливість онлайн-ресурсів для комерційних та державних організацій і регулярно роблять спроби злому за допомогою атак на відмову в обслуговуванні, метою яких є порушення їх працездатності. Такі DoS/DDoS-атаки можуть здійснювати як звичайні зловмисники, вимагаючи сплати за припинення атак, так і недобросовісні компанії, які намагаються причинити шкоду або загальмувати розвиток бізнесу компанії-конкурента.



infocom
TRUSTED SECURITY

Одним із найпоширеніших методів такої кібератаки є насичення інфраструктури клієнта великою кількістю зовнішніх запитів таким чином, що атаковане устаткування не може відповісти справжнім користувачам, або відповідає настільки повільно, що стає, фактично, недоступним. Як правило, відмова атакованого сервісу досягається шляхом:

- примусу до повної зупинки роботи програмного забезпечення/устаткування атакованого сервісу, або до витрат наявних апаратних ресурсів, внаслідок чого устаткування не може продовжувати роботу
- перевантаження комунікаційних каналів між користувачами і атакованим сервісом, внаслідок чого швидкість передачі даних припиняє відповідати будь-яким вимогам для забезпечення нормального функціонування відповідного веб-порталу

Послуга infoDDoS може протистояти всім відомим типам DoS/DDoS-атак та забезпечує безперервну роботу Ваших ресурсів в мережі «Інтернет» за допомогою багаторівневого захисту у який входить увесь спектр сучасних засобів протидії атакам на відмову в обслуговуванні. У перелік засобів окрім поведінкового захисту, обмеження одночасних з'єднань, обмеження трафіку, захисту від SYN-флуду та інших, входить вбудована система запобігання зовнішнім вторгненням, яка є високопродуктивним методом протидії атакам з використанням відомих вразливостей програмного забезпечення, яке може використовуватися на вашому веб-порталі. Крім цього, платформа послуги infoDDoS дозволяє уникнути ризиків проникнення «комп'ютерних черв'яків» та з легкістю виявляє роботу «ботів» на комп'ютерах співробітників.

Технології та засоби захисту послуги infoDDoS

- Поведінковий захист забезпечує захист від атак на основі аналізу поведінки трафіку. Система виявляє аномальні шаблони поведінки трафіку та приймає необхідні заходи для його блокування.
- Система запобігання вторгнень забезпечує виявлення та блокування вторгнень у реальному часі. Вона використовує бази даних з відомими вразливостями та шаблонами атак для виявлення небезпечного трафіку та його блокування.
- Захист від SYN-флуду забезпечує захист від атак, що спрямовані на використання ресурсів мережі шляхом надмірного використання SYN-пакетів.
- Обмеження одночасних з'єднань забезпечує обмеження кількості одночасних з'єднань для кожної IP-адреси, що намагається отримати доступ до захищеного ресурсу.
- Обмеження трафіку дозволяє контролювати обсяг вхідного трафіку. Це допомагає позбавитися надмірної завантаженості, через надмірну кількість запитів.
- Технологія SPI використовується для виявлення потенційно небезпечних пакетів даних. Вона дозволяє встановлювати зв'язок між пакетами, що забезпечує більш точний аналіз трафіку та виявлення небезпечних запитів.
- Захист від сканування портів дозволяє виявляти та блокувати спроби сканування відкритих портів на захищеному ресурсі.
- Захист від http-флуду дозволяє виявляти та блокувати спроби перевантаження веб-ресурсу запитами.

Послуга infoDDoS це:

- Безперервна робота ваших ресурсів у мережі «Інтернет»
- Зниження ризиків порушення діяльності вашої Компанії
- Оптимізація ваших витрат на забезпечення захисту від DoS/DDoS-атак завдяки відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього
- Економія вашого часу та можливість повністю сконцентруватись на ваших стратегічних планах та задачах
- Залучення фахівців Infocom без необхідності у додатковому навчанні власних
- Моніторинг і контроль атак та інцидентів 24x7x365

infocom
TRUSTED SECURITY