Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-net-ddos

SIECI KOMPUTEROWE

DoS i DDoS, czyli jak zakorkować autostradę bez jednego wypadku

Na Autostradzie Pakietów jest piękny poranek. Samochody jadą, bramki pobierają opłaty, routery kierują ruchem, a kierownik **NAT** właśnie odnalazł swój zeszyt. Niestety, nie ten.

Wszystko działa. Aż do chwili, kiedy przed jedną z bramek zatrzymuje się samochód.

— Dzień dobry. Czy można zapłacić kartą?
— Można.
— A gotówką?
— Też można.
— A kartą?
— Przed chwilą pan pytał.
— A gotówką?
— Panie, za panem jest kolejka!
— Rozumiem. A kartą można?

Kasjer zaczyna podejrzewać, że kierowca nie zamierza nigdzie jechać. I rzeczywiście. Ten kierowca nie przyjechał po to, żeby skorzystać z autostrady. **Przyjechał po to, żeby nikt inny nie mógł z niej korzystać.**

DoS, czyli jeden bardzo upierdliwy klient

DoS oznacza *Denial of Service*, czyli odmowę dostępu do usługi. Nie chodzi o to, że serwer obraził się na użytkownika. Chodzi o doprowadzenie do sytuacji, w której prawidłowi użytkownicy nie mogą korzystać z usługi albo korzystanie z niej jest poważnie utrudnione.

Na naszej autostradzie jeden kierowca może blokować bramkę niekończącymi się pytaniami. W sieci przyczyną może być przeciążenie zasobów albo wykorzystanie błędu w sposobie obsługi żądań.

Atak nie musi nawet generować ogromnego ruchu. Czasem wystarczy, że usługa zostanie zmuszona do wykonywania wyjątkowo kosztownych operacji.

— Czy może pan sprawdzić historię wszystkich przejazdów od 1997 roku, posortować według nazwiska panieńskiego właścicieli pojazdów i wydrukować w trzech egzemplarzach?
— Ale po co?!
— Bo mam takie prawo!
— A nie może pan po prostu zapłacić pięciu złotych?!
— Najpierw poproszę raport.

Kasjer znika w archiwum na pół godziny. Tymczasem autostrada stoi.

DDoS, czyli zjazd rodzinny na sto tysięcy samochodów

Administrator autostrady wysyła ochroniarza. Ochroniarz podchodzi do kierowcy i oznajmia:

— Pan już dzisiaj nie przejedzie.
— Dobrze.

Samochód odjeżdża. Kolejka rusza. Przez jakieś cztery sekundy. Potem na autostradę wjeżdża sto tysięcy samochodów. Każdy zatrzymuje się przed bramką. Każdy opuszcza szybę. Każdy pyta:

— Czy można zapłacić kartą?

🤣 To już **DDoS — Distributed Denial of Service**, czyli rozproszony atak powodujący niedostępność usługi. Najważniejsza różnica polega na tym, że atak pochodzi z wielu rozproszonych źródeł.

Często są nimi urządzenia należące do botnetu — komputerów, serwerów, routerów, kamer czy innych urządzeń przejętych przez atakujących. Właściciele nie muszą nawet wiedzieć, że ich sprzęt bierze w tym udział.

Wyobraźmy sobie kamerę pilnującą podjazdu. Przez większość dnia obserwuje samochód właściciela, a między nagraniami pomaga blokować autostradę po drugiej stronie kontynentu.

— Panie kierowniku, kamera z magazynu bierze udział w ataku!
— Która?!
— Ta nad bramą.
— Przecież ona nawet nie ma kół!
— Ale ma Internet.

Trzy sposoby na zrobienie korka

Nie każdy atak DoS lub DDoS wygląda tak samo. Na Autostradzie Pakietów można sparaliżować ruch na kilka zupełnie różnych sposobów.

1. Zatkanie całej autostrady

Pierwszy sposób jest brutalnie prosty: tyle ruchu, że łącze nie jest w stanie go pomieścić. Jeśli droga obsługuje tysiąc samochodów na minutę, a próbuje nią przejechać dziesięć tysięcy, nie pomoże nawet najszybszy kasjer.

Samochody stoją wiele kilometrów przed bramkami. Serwer docelowy może mieć mnóstwo wolnej pamięci i prawie bezczynny procesor. Tylko co z tego? **Pakiety nawet do niego nie docierają.**

Administrator ogląda monitoring.

— CPU pięć procent. RAM trzydzieści procent. Dyski się nudzą.
— To dlaczego usługa nie działa?!
— Bo wejście na parking jest czterdzieści kilometrów stąd, a kolejka już sięga Czech.

To przykład ataku wolumetrycznego — jego celem jest przede wszystkim przepustowość sieci.

2. Zajęcie wszystkich stanowisk obsługi

Drugi sposób polega na przeciążaniu mechanizmów obsługi ruchu i połączeń. Bramki stoją, kasjerzy pracują, ale każde stanowisko jest zajęte.

Urządzenia sieciowe i serwery mają ograniczone zasoby potrzebne między innymi do utrzymywania stanów połączeń. Ich wyczerpanie może utrudnić obsługę prawidłowych klientów.

— Następny!
— Chciałbym rozpocząć procedurę płatności.
— Dobrze, proszę podać kartę.
— Jeszcze nie.
— To może gotówkę?
— Też nie.
— To na co pan czeka?!
— Na rozpoczęcie kolejnej procedury.

Za nim stoi pięć tysięcy identycznych samochodów.

Przykładem historycznie znanego ataku tego rodzaju jest **SYN flood**, choć współczesne systemy mają mechanizmy ograniczające skuteczność wielu jego odmian. O połączeniach **TCP** opowiadaliśmy szerzej w artykule **TCP i UDP**.

3. Zajechanie urzędu papierologią

Trzeci sposób to przeciążenie warstwy aplikacyjnej. Żądania mogą przypominać zwykły ruch użytkowników i wcale nie muszą zajmować wielkiej przepustowości. Wystarczy, że każde kosztuje serwer sporo pracy.

— Poproszę zestawienie wszystkich faktur.
— Za jaki okres?
— Za cały.
— W jakiej kolejności?
— Według kwoty, daty, a potem jeszcze raz kwoty.
— Dobrze…
— A teraz od początku, ale odwrotnie.

Po chwili przychodzi kolejny petent. I następny. I jeszcze dziesięć tysięcy kolejnych.

Łącze działa. Serwer odpowiada. Tylko prawdziwi klienci nie mogą się dopchać.

Dlaczego nie wystarczy zablokować adresów IP?

Kierownik ochrony wpada do serwerowni.

— Mam rozwiązanie!
— Jakie?
— Zablokujemy wszystkich!
— Wszystkich atakujących?
— WSZYSTKICH!

— Ale wtedy nikt nie skorzysta z usługi.
— Za to nikt jej nie zaatakuje!
— Czyli sam pan właśnie zrobił DoS.

🤣 Najtrudniejsze jest odróżnienie niepożądanego ruchu od prawidłowego. Przy rozproszonym ataku blokowanie pojedynczych adresów może niewiele dać, bo źródeł bywają tysiące. Niektóre ataki wykorzystują też podszywanie się pod adresy nadawców.

Z kolei zbyt agresywne filtrowanie może odciąć niewinnych użytkowników. **Bezpieczeństwo**, które polega na zamknięciu usługi dla wszystkich, ma pewne istotne wady.

Czy większy serwer rozwiąże problem?

— Panie kierowniku, kupiliśmy nowy serwer!
— Jaki?
— Sześćdziesiąt cztery rdzenie, pół terabajta RAM-u, dyski NVMe!
— Świetnie. A łącze?
— To samo.
— Czyli?
— Korek nadal zaczyna się czterdzieści kilometrów przed bramką.

Większa moc pomaga, gdy problemem są zasoby serwera. Jeśli zapchane jest łącze, filtr działający dopiero na serwerze może być bezsilny.

Dlatego ochrona przed dużymi atakami często wymaga działania wcześniej: u operatora, w wyspecjalizowanej infrastrukturze filtrującej albo w usługach rozproszonych. Pomocne bywają ograniczenia liczby żądań, wykrywanie anomalii, CDN-y i usługi ochrony DDoS. **Nie istnieje jeden magiczny przełącznik odporny na wszystko.**

A może to wcale nie atak?

Na Autostradzie Pakietów nagle pojawia się ogromny korek. Administrator sprawdza wykresy.

— Ruch wzrósł dwudziestokrotnie!
— DDoS?!
— Niekoniecznie.
— Botnet?!
— Niekoniecznie.
— Rosyjscy hakerzy?!
— Uspokój się.

Po chwili okazuje się, że popularny portal opublikował link do strony. Tysiące prawdziwych użytkowników próbują odwiedzić ją jednocześnie.

Nie każde przeciążenie jest atakiem. Objawy mogą być podobne: opóźnienia, błędy, brak odpowiedzi. Ale przyczyna i sposób reagowania są inne. Jeden wykres nie wystarczy, żeby postawić diagnozę.

— Czyli to nie atak?
— Nie. Po prostu staliśmy się popularni.
— To dobrze?
— Zależy, czy zdążymy zwiększyć pojemność parkingu.

Finał: bezpieczeństwo absolutne

Po całym dniu walki z DDoS kierownik autostrady zwołuje zebranie.

— Panowie, mam plan, który definitywnie rozwiąże problem.
— Słuchamy.
— Zamykamy autostradę.

Cisza.

— Na jak długo?
— Na stałe.
— Ale wtedy nikt nie będzie mógł przejechać!
— Właśnie. I żaden atak już nas nie przeciąży.

Administrator spogląda na kierownika.

— Gratuluję. Właśnie osiągnął pan stuprocentową skuteczność ataku DoS na własną infrastrukturę.
— Dziękuję.
— To nie był komplement.

🤣