**Kraków, 21.06.2018r.**

**Nazwa.pl powstrzymuje atak DDoS**

**We wtorek, 19 czerwca 2018 r., miał miejsce jeden z największych ataków DDoS w polskim Internecie na infrastrukturę DNS firmy nazwa.pl, lidera usług hostingowych w Polsce. Incydent ten utrudnił Klientom spółki korzystanie z usług WWW i poczty. Atak DDoS jest najczęstszą formą stosowaną w celu zaburzenia funkcjonowania systemów sieciowych i może dotknąć każdego dostawcę usług. Administratorzy systemów nazwa.pl powstrzymali incydent, wykorzystując do tego narzędzia sieciowe wsparte najnowszym wdrożeniem, czyli technologią serwerów DNS Anycast.**

DDoS - skrót od ang. Distributed Denial of Service – to rozproszony atak, który ma na celu zatrzymanie prawidłowego funkcjonowania usługi lub spowodowanie odmowy jej działania. Atak tego typu generuje sztuczny ruch tak, aby wykorzystać wszystkie wolne zasoby serwerów i doprowadzić do niedostępności usług. Do przeprowadzenia ataków służą między innymi botnety, czyli grupy komputerów zainfekowanych [szkodliwym oprogramowaniem](https://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie), pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi zarażonymi komputerami. Wykorzystanie przez przestępców zainfekowanych komputerów czyni źródło ataku DDoS niemożliwym do zlokalizowania, a wyśledzenie jego sprawców jest praktycznie niemożliwe.

Ataki typu DDoS są jednym z największych problemów współczesnego Internetu, a ich skala rośnie z roku na rok. W ostatnim czasie spada średni czas trwania ataku DDoS. Obecnie najczęściej trwa on poniżej 30 minut, jednak mimo to nadal zdarzają się incydenty trwające nawet kilka dni. W przypadku ataku na serwery nazwa.pl, zdarzenie podzielone było na dwa etapy trwające: 30 minut – pierwszy incydent i 2 h i 20 minut – drugi incydent. Po zakończeniu głównego ataku pojedyncze boty atakowały system do końca dnia. W wyniku zdarzenia ruch na serwerach wzrósł dwudziestokrotnie w porównaniu z godzinami szczytu występującymi podczas codziennego funkcjonowania systemu.

Podczas wtorkowego zdarzenia administratorzy systemów nazwa.pl rozłożyli sztucznie generowany ruch na dodatkowe klastry serwerów utworzonych w wyniku migracji serwerów DNS do technologii Cloud – chmury. Dzięki temu serwery zostały połączone w klastry, dając możliwość szybkiego skalowania zasobów. Takie rozwiązanie pozwala na zwiększenie dostępnych zasobów w odpowiedzi na nagły wzrost sztucznego ruchu będącego wynikiem ataków generowanych przy pomocy wspomnianych wcześniej botnetów. Już w obecnej konfiguracji technologia serwerów DNS Anycast zastosowana w nazwa.pl jest w stanie obsługiwać kilka milionów zapytań na sekundę, co redukuje do minimum możliwość przeprowadzania podobnego ataku w przyszłości.

Nazwa.pl intensywnie pracuje od początku roku nad wdrożeniem technologii serwerów DNS Anycast w kluczowych globalnych punktach wymiany ruchu, migrując 13.czerwca 2018r. domeny Klientów na nową technologię w Data Center zlokalizowanych w Krakowie i w Warszawie. Wtorkowe zdarzenie pozwoliło zweryfikować pilotażowe polskie wdrożenie w warunkach realnego ataku, co w efekcie znacząco przyczyniło się do jego powstrzymania. Z jednej strony zdarzenie utwierdziło firmę w przekonaniu o słuszności dokonanego wyboru, a z drugiej - zdeterminowało największego dostawcę usług internetowych w Polsce do rozszerzenia wdrożenia DNS Anycast najpierw na teren Europy, a następnie na kolejne kontynenty, dzięki czemu nazwa.pl, jako pierwsza firma w Polsce, osiągnie całkowitą georedundancję serwerów. Rozwiązanie zapewni Klientom z różnych rejonów świata lokalny dostęp do serwerów DNS utrzymujących informacje o domenach Klientów nazwa.pl. Takie rozwiązanie nie tylko dodatkowo zabezpieczy Klientów przed atakami DDoS, ale również znacząco przyspieszy działanie stron WWW, które będą błyskawicznie dostępne z dowolnego punktu na Ziemi. Technologia DNS Anycast stosowana jest przez największe firmy na świecie, a nazwa.pl będzie pierwszą firmą w Polsce, która wdroży to rozwiązanie, wyprzedzając znacznie technologie stosowane przez rodzime firmy.

Strategia nazwa.pl oparta jest o trzy filary związane z bezpieczeństwem. W ich zakres wchodzą rozwiązania infrastrukturalne, systemowe i prawne. Firma, wdrażając technologię serwerów DNS Anycast, ma na celu zwiększenie poziomu bezpieczeństwa infrastrukturalnego, a co za tym idzie zminimalizowania podatności na ataki DDoS w przyszłości. Mimo, że ryzyko powtórzenia takich ataków istnieje i dotyczy wszystkich firm hostingowych w Polsce i na świecie, nazwa.pl dzięki precyzyjnie przygotowanemu wdrożeniu technologii serwerów DNS Anycast będzie przygotowana na tego typu incydenty najlepiej ze wszystkich polskich firm hostingowych . Nazwa.pl – firma nr 1 w Polsce – wchodzi w ten sposób do światowej czołówki, a głównymi beneficjentami stają się Klienci spółki, którzy chronieni będą przy użyciu najbardziej zaawansowanych, światowych rozwiązań w tej dziedzinie.