# Największy atak hackerski w historii Internetu

29 marca 2013

Spam to utrapienie Internetu. Wie o tym każdy administrator, który zmaga się z hordami automatów spamujących. Na wielką skalę jest też wysyłany na nasze skrzynki mailowe i dlatego istnieją firmy takie jak Spamhaus, która pomaga dostawcom poczty e-mail z radzeniem sobie z problemem niechcianej korespondencji. To właśnie Spamhaus stał się ofiarą największego ataku hackerskiego typu DDoS w historii Internetu.

Ataki typu DDoS polegają na tym, że na dany serwer jest wysyłana duża ilość zapytań, wielokrotnie przekraczająca jego możliwości. W rezultacie dochodzi do przeciążenia serwera i dany serwis czy też strona internetowa po prostu przestaje działać. Na takie ataki nie ma rady, po prostu się zdarzają i trzeba je przetrwać. Do wzmocnienia ich siły stosuje się czasami serwery DNS i wtedy ofiara ma poważne kłopoty. Dokładnie tak było w przypadku Spamhaus.

Firma ta poprzez rolę, jaka pełni ma dość dużą władzę i czasami może wciągnąć na czarną listę adresy IP serwerów niekoniecznie zajmujących się spamem. Taki spór Spamhaus toczył ostatnio z holenderską firmą CyberBunker specjalizująca się w hostowaniu wszystkiego poza pornografią dziecięcą i terroryzmem. Data center znajduje się w dawnym bunkrze atomowym, stąd nazwa. To właśnie CyberBunker był początkowo podejrzewany o atak przepuszczony na Spamhaus. Prezes Sven Olaf Kanphuis stanowczo jednak się od tego odcina.

Atak przeprowadzony na Spamhaus był tak ogromny, że mógł doprowadzić do przeciążenia routerów brzegowych u operatorów tak zwanego Tier, 1 czyli zarządzających ruchem w sieci Internet. DDoS o wielkości nawet 300 Gb/s to potężne

obciążenie dla interfejsów i nawet jeśli ISP w drugiej warstwie wycina ruch przychodzący to w Tier 1 on nadal istnieje i prowadzi z czasem do przeciążania interfejsów. Ostatecznie atak na Spamhaus trwał ponad tydzień a serwisy firmy przetrwały pozostając online, ale stało się tak tylko dlatego, że swojego klienta ostatkiem sił obroniła firma CloudFlare specjalizująca się w przyspieszaniu i zabezpieczaniu serwerów internetowych.

Cyberataki stają się ostatnio coraz częstsze. Kilka dni temu przestała działać część sieci komputerowej południowokoreańskich banków. Kilka lat temu rosyjscy hakerzy skutecznie DDoSowali banki w Estonii. Chińscy hakerzy stają się tak agresywni, że Pentagon zastanawia się jak odpowiadać na kolejne ataki. Internet staje się polem walki i to nie tylko między firmami, między obywatelami a władzą, ale również między krajami. Niewiele osób wie, że w zeszłym roku wprowadzono w Polsce prawo, które pozwala prezydentowi na wprowadzenie stanu wyjątkowego na terenie kraju gdyby doszło do wielkiego cyberataku.

Widząc skalę i czas trwania ataku można powiedzieć, że Internet jest zagrożony. Wygląda na to, że przeciążenie routerów brzegowych jest o wiele łatwiejsze niż dotychczas sądzono a to oznacza nie tylko, że podczas takiego ataku cały Internet może znacznie zwolnić, ale również oznacza prawdopodobne długotrwałe przerwy w dostępie do zasobów światowej sieci.

Na podstawie: arstechnica.com
Źródło: Zmiany na Ziemi