DDOS – ZAPOMNIANE ZAGROŻENIE [ANALIZA]

Ataki DDoS stały się sławne za sprawą wykorzystania ich jako broni politycznej przeciwko Estonii w 2007 roku i 2008 w Gruzji. Jest to jeden z najpopularniejszych rodzajów ataku używanych przez haktywistów, cyberprzestępców czy służby specjalne państw. Dzisiaj staję się na tyle powszechne, że praktycznie każdy może sobie pozwolić na ich wykorzystanie.

Czym są ataki DDoS?

Ataki typu rozproszona odmowa usługi (Denial Distributied of Services – DDoS) polegają na przeprowadzeniu operacji wymierzonej w system komputerowy lub usługę sieciową, której celem jest zajęcie wszystkich wolnych zasobów. Przeprowadzony jest on z wielu komputerów jednocześnie. Dlatego też do przeprowadzenia DDoS często wykorzystywane są botnety, złożone z tysięcy zainfekowanych wcześniej komputerów nad którymi zdalną kontrolę przejmuje haker i każe im połączyć się z danym serwerem w tym samym czasie. Pierwsze botnety powstały w 1993 roku i były kontrolowane przez przesyłane przez IRC komunikaty. Ataki DDoS są jednak jeszcze starsze. Pierwszą tego typu operacje odnotowano w 1974 roku. Przez przypadek dokonał tego 13 latek w stanie Illionois.

Czytaj też: Raport: 28 proc. wzrost liczby ataków DDoS

Wybrane ataki DDoS

DDoS są używane na wielu różnych sposób. Pierwszym z nich jest ich wykorzystanie jako politycznego narzędzia przez służby innych krajów i haktywistów. W 2007 roku w stolicy Estonii Tallinnie podjęto decyzję o przeniesieniu tzw. Brązowego Żołnierza, który upamiętniał radzieckich wojskowych poległych w bitwie o to miasto. Ze strony rosyjskiej rozległy się głosy oburzenia, na ulice Tallina wyszli miejscowi Rosjanie, potężne protesty miały też miejsce w Moskwie przed ambasadą Estonii. Równolegle w cyberprzestrzeni rozpoczęła się operacja, której celem były strony administracji rządowej, banków i agencji prasowych. Kraj tak silnie uzależniony od internetu został jako pierwszy zaatakowany w cyberprzestrzeni. Estoński rząd sondował nawet możliwość powołania się na artykuł V Traktatu Waszyngtońskiego o kolektywnej obronie, ale sojusznicy z NATO nie chcieli się zgodzić. Ponadto brakowało procedur reagowania na cyberataki i większość decydentów nie wiedziała, jak mają postąpić. Należy również podkreślić, że ataki DDoS nie miały aż tak druzgocącego skutku jak początkowo je przedstawiano. Skutki naprawy szkód nie były wielkie i zamknęły się w sumie kilku milionów euro. Termin cyberwojny tak powszechnie stosowany do opisu tych ataku nie znajduję tutaj zasadności. Operacji wymierzonej w Estonię bliżej było do cyberwandalizmu a nie konfliktu militarnego. Jednak to właśnie ataki DDoS z 2007 roku powszechnie postrzega się jako bodziec, który zdynamizował dyskusję o cyberbezpieczeństwie i rozpoczął proces zmian i reform NATO i Unii Europejskiej w tej sferze.

Ataki DDoS zostały również wykorzystany w trakcie trwania działań militarnych w Gruzji w 2008 roku.

Pierwsze ataki zostały przeprowadzone jeszcze przed 7 sierpnia 2008 roku, czyli dniem wyznaczającym początek wojny. Jest to kolejny dowód świadczący o rosyjskiej planowanej agresji a nie spontanicznej odpowiedzi na atak gruziński, tak jak niektórzy chcieliby to widzieć. W ataki DDoS zaangażowano każdego, który chciał wesprzeć Rosję w tej wojnie. Na rosyjskojęzycznych forach można było ściągnąć program do przeprowadzania ataku DDoS zatytułowany „Niskoorbitalne Działo Jonowe" (Low Orbit Ion Cannon) wraz z instrukcją obsługi, co powodowało, że nawet użytkownicy nie posiadający dużej wiedzy informatycznej byli w stanie uczestniczyć w ataku na Gruzję.

Czytaj też: Rosjanie i Chińczycy autorami zmasowanego ataku DDoS

Ataki DDoS były nie tylko wykorzystywane przez państwa przeciwko innym krajom, ale równie często przez grupy haktywistów. Ich częstym celem był kontrowersyjny kościół scjentologów, ale nie tylko. W 2012 roku podczas protestów przeciwko porozumieniu ACTA, rozpoczął się szereg ataków na polskie instytucje parlamentarne i rządowe. Miały one zostać dokonane przez grupę Anonymous, która bardzo często wykorzystuje tę metodą w swoich działaniach. Strony Sejmu czy niektórych instytucji rządowych były czasowo niedostępne. Pokazało to całkowity brak przygotowania polskiej administracji na takie wyzwania. Nie był to zresztą pierwszy atak na polskie instytucje. Wcześniej ich celem był m.in. portal Gazeta.pl czy serwis Policja.pl.

DDoS wykorzystywane są również do szantażowania firm, serwisów aukcyjnych, firm brokerskich i innych, gdzie przerwanie w działaniu systemu transakcyjnego bezpośrednio przekłada się na straty finansowe firmy i jej klientów. Takie działania jest niezgodne z prawem. Celem były również gry online w całej Europie jak np. stardoll.com. Ataki DDoS były również wymierzone w 13 głównych serwerów DNS obsługujących tłumaczenie nazw domen na adresy IP. Pierwszy z nich nastąpił w 2002 roku, doprowadzając do blokady dziewięciu z nich, a drugi w 2007, kiedy dwa zostały zablokowane.

Rozwiązania związane z internetem rzeczy stwarzają nowe możliwości dla ataków DDoS. Najlepszym przykładem jest tutaj botnet Mirai złożony z urządzeń IoT. Doprowadził on do największych ataków DDoS w historii wymierzonych w stronę znanego dziennikarza Briana Krebsa o sile 665 gigabitów na sekundę, stronę francuskiej firmy hostingowej OVH i przede wszystkim ataku na serwery firm Dyn, zarządzającej usługami DNS wielu popularnych internetowych serwisów co doprowadziło do poważnych problemów z dostępem do wielu usług takich jak: Twitter, Etsy, Github, SoundCloud, Spotify, Heroku, Pagerduty czy Shopify, które korzystały z usług tego samego dostawcy DNS czyli firmy Dyn. Był to rekordowy co do wielkości ataku przeprowadzony ze 100 tys. urządzeń o sile 1.2 terabitów na sekundę. Według ekspertów, te wartości w przyszłości mogą być jeszcze większe.

Według Jakuba Syty Dyrektora Biura Zarządzania Usługami Bezpieczeństwa EXATEL obserwowane ataki DDoS najczęściej dotykają 3 i 4 warstwy modelu OSI (warstwy sieciowej i transportowej), choć można również zaobserwować ataki wolumetryczne wykorzystujące podatności na warstwie 7 - aplikacyjnej. Potężne ilości zapytań, na które trzeba odpowiedzieć, stają się w którymś momencie niemożliwe do obsłużenia. Źródłem ataku najczęściej są farmy przejętych komputerów nieświadomych użytkowników, choć coraz częściej można obserwować ataki, których źródłem są przejęte urządzenia. Świat IoT, określany niekiedy złośliwie jako „insecurity by design" jest z tego właśnie powodu bardzo atrakcyjny dla przestępców.

Czytaj też: Kamery przemysłowe wykorzystane do ataku DDoS

Pomimo, że obecnie ataki typu DDoS znajdują się w cieniu Ransomware, który przyciąga główną medialną uwagę, to ich popularność nie maleje, a wręcz przeciwnie stają się one ogólnodostępną usługą, dla praktycznie każdego kogo stać, żeby zapłacić odpowiednią sumę pieniędzy.

DDoS jako usługa

Ostatnio portal SCMagazine donosił o przypadku Amerykanina, który opłacał hakerów do przeprowadzania ataku DDoS wymierzonego w jego byłych pracodawców i inne firmy. John Kelsey Gammel został oskarżony o celowe spowodowanie uszkodzeń chronionych komputerów. Jeżeli zostanie skazany grozi mu od 15 do 17 lat pozbawienia wolności. Przykład Gammela pokazuje, że ataki DDoS są już stosowane przez zwykłych obywateli, którzy przykładowo szukają zemsty. Z badań przeprowadzonych przez Neustar wynika, że dwie trzecie największych firm było ofiarami ataku DDoS, a codziennie dochodzi do prawie 4 tys. tego typu operacji na całym świecie. To natężenie cyberataków możliwe jest dzięki zwiększające się liczbie niezabezpieczonych lub źle zabezpieczonych urządzeń IoT, do których bardzo łatwo się włamać. Prowadzi to do sytuacji, że coraz częściej ataki DDoS oferowane są jako usługa na tzw. podziemnych cyberynkach.

Właściciele botnetów oferują za niewielką opłatą ich wynajęcie do przeprowadzenia ataków. Cena uzależniona jest od czasu ataku, częstotliwości przeprowadzania oraz jego wielkości i waha się od 20 dolarów do 500 dolarów miesięcznie. Większość sprzedających akceptuję jedynie bitcoiny, ale zdarzają się oferty za które można zapłacić za pomocą PayPala. Ataki DDoS sa również bardzo popularne ponieważ trudno jest zlokalizować ich źródło i złapać potencjalnych sprawców. Wyżej opisana sprawa oskarżonego Amerykanina jest wyjątkiem. Biorąc pod uwagę rosnące zagrożenie spowodowane atakami DDoS należy rozważyć szereg środków ochronnych, które mogą zmniejszyć skutki takich operacji.

Jakub Syta Dyrektor Biura Zarządzania Usługami Bezpieczeństwa EXATEL komentuje, że ataki DDoS są realnym zagrożeniem dla wszystkich, którzy świadczą usługi przez Internet. Zablokowanie ich działalności na okres godzin czy dni nie wymaga znacznych nakładów a przekłada się na realne straty biznesowe. Z tego też powodu jest często wykorzystywane przez nieuczciwych konkurentów oraz szantażystów. Czarny rynek kwitnie – możliwe jest wręcz zakupienie ataków na godziny po bardzo okazyjnych cenach.

Sposoby ochrony przed atakami DDoS?

Według Jakuba Syty pojedyncze przedsiębiorstwa mają bardzo ograniczone możliwości skutecznej reakcji. Rzeczywistą ochronę mogą dać jedynie rozwiązania klasy operatorskiej, pozwalające na rozproszenie ruchu i jego wyczyszczenie ze sfałszowanych połączeń, zanim dotrą one do celu. Istotą tzw. mitygacji jest to by wyfiltrować ruch niepożądany, lecz pozwolić na normalne funkcjonowanie usług, choć najprostsze z usług po prostu polegają na kontrolowanym odcięciu całego ruchu do zaatakowanej organizacji. Nie każda z organizacji akceptuje jednak tego typu rozwiązania.

Czytaj też: 5 mitów na temat ataków DDoS [ANALIZA]

Zakończenie

Ataki DDoS ze względu na swoją skuteczność oraz niewielkie koszty będą coraz popularniejsze. Ten trend będzie potęgowany przez dostępność usług i narzędzi umożliwiających takie operacje coraz większej ilości użytkowników, którzy niekoniecznie muszą posiadać wyspecjalizowane umiejętności. Ponadto rosnąca liczba, niezabezpieczonych urządzeń IoT powoduje, że rozmiar ataków będzie tylko większy, co może doprowadzić do czasowego paraliżu najważniejszych systemów.