CO TO JEST ATAK DDoS

I JAK SIĘ PRZED NIM CHRONIĆ?

DATASPACE

Spis treści

Spis treści

Spis treści

Cześć I.
Podstawy

Co to jest DDoS?

Skrót **DDoS** pochodzi od angielskiego określenia *distributed denial of service*, co można przetłumaczyć jako **rozproszona odmowa dostępu**. To jedna z wielu metod wykorzystywanych do blokowania internetowych serwisów lub blokowania łączy internetowych.

Jakie są rodzaje ataków DDoS?

Są 2 podstawowe rodzaje ataków DDoS:

- **atak wolumetryczny** – atak polegający na masowej wysyłce niechcianych danych na wskazany adres IP; ilość napływających danych jest tak duża, że łącze (lub łącza) internetowe nie są w stanie przyjąć tych wszystkich danych,
- **atak aplikacyjny** – atak polegający na wyczerpaniu zasobów informatycznych aplikacji internetowej, np. mocy obliczeniowej lub pamięci; czasami ataki tego typu nazywane są atakami typu *slow*.

Na czym polega atak DDoS?

Wyobraź sobie sklep, do którego prowadzą jedne drzwi wejściowe. Drzwi mają swoją przepustowość, ponadto jak każde wejście do sklepu wyposażone są w systemy antykradzieżowe oraz monitorowane są przez pracowników ochrony. Jak wyglądałaby analogia sytuacji naszego sklepu do każdego z wyżej wymienionych typów ataków DDoS?

Spis treści

Wolumetryczny atak DDoS można przyrównać do sytuacji, gdy do sklepu próbuje wejść, w tej samej chwili, bardzo duża liczba osób. Co ważne, znacząca większość z tych osób nie ma zamiaru robić żadnych zakupów, ich celem jest raczej zrobienie sztucznego tłoku przy wejściu i zablokowanie wejścia do sklepu. Efektem takiego działania jest problem z dostaniem się do środka rzeczywistych Klientów, którzy chcą zrobić zakupy. Problemy mają również klienci, którzy próbują wyjść z takiego sklepu – oni również nie mogą wydostać się, poprzez zablokowane natłokiem ludzi, drzwi wejściowe.

Ponadto ochrona sklepu ma całą masę roboty, ponieważ próbuje zapanować nad tłumem, jednocześnie praktycznie nie jest w stanie sprawdzać, co jest wnoszone do sklepu, a tym bardziej wynoszone ze sklepu.

Podobnie jest w przypadku ataku na aplikację internetową. Z całego świata wysyłane są pakiety danych, które docierają do łącza internetowego ofiary, w którym nie są w stanie się zmieścić. Tym samym zablokowana zostaje komunikacja aplikacji internetowej z Internetem. Dane ze świata nie są w stanie przebić się przez natłok niepotrzebnych pakietów, podobnie jest z wysyłaniem informacji – które nie mogą być wysłane, z uwagi na zablokowane łącze internetowe. W praktyce można przyrównać to do sytuacji, gdy łącze internetowe ulega awarii. W przypadku ataku wolumetrycznego łącze internetowe jest sprawne, jednak jego wydajność jest zbyt mała, aby obsłużyć transmisję napływających danych. Dodatkowo problem powiększa kwestia utraty kontroli nad ochroną. Nadmiar danych sprawia, że systemy ochrony (firewall) nie są w stanie obsłużyć wszystkich danych, a tym bardziej ich przeanalizować. W zależności od konfiguracji, firewall blokuje obsługę kolejnych sesji internetowych lub wyłącza ochronę i przepuszcza wszystkie sesje, jakim tylko uda się przebić przez natłok danych.

Spis treści

Atak aplikacyjny

Wykorzystując powyższy przykład ze sklepem, **atak aplikacyjny** można porównać do niepotrzebnego angażowania obsługi sklepu. Wyobraźmy sobie, że weszliśmy do sklepu i potrzebujemy pomocy sprzedawcy, aby dokonać ostatecznego wyboru, otrzymać towar z odpowiednim rozmiarze czy kolorze. Atakujący w tym wypadku mają za zadanie maksymalne zaangażowanie czasu sprzedawcy. Na przykład, dopytują sprzedawcę o mało istotne szczegóły, przerywają mu rozmowę z rzeczywistym Klientem, awanturują się - mówiąc krótko - robią niepotrzebne zamieszanie, nie po to aby cokolwiek kupić, ale po to aby spowolnić lub nawet uniemożliwić pracę sprzedawców. Odpowiednio duża liczba takich „klientów-pieniaczy" jest w stanie zniechęcić rzeczywistych Klientów do zakupów.

A jak to wygląda w przypadku systemów informatycznych? Atak aplikacyjny (typu *slow*) powoduje, że serwis internetowy otrzymuje całą masę zapytań, gdzie jednocześnie wydłużony jest maksymalnie czas odpowiedzi ze strony pytającego. W praktyce oznacza to tyle, że każda aplikacja internetowa rozpoczynając nową sesję internetową (np. z przeglądarką użytkownika), rezerwuje mały procent zasobów informatycznych, potrzebnych do obsługi tej sesji. Jednocześnie, każda sesja internetowa posiada pewien zestaw reguł typu „pytanie-odpowiedź", gdzie ustalony został maksymalny czas oczekiwania na „odpowiedź". Przez cały czas oczekiwania na „odpowiedź" zasoby informatyczne zarezerwowane dla danej sesji są utrzymywane w gotowości i nie mogą służyć do obsługi innych procesów informatycznych.

Odpowiednio duża liczba otwieranych sesji, które „odpowiadają" z maksymalną, dopuszczalną zwłoką sprawia, że zasoby informatyczne mogą ulec wyczerpaniu. Pierwszym objawem zaatakowanej aplikacji jest spowolniona obsługa, co w praktyce oznacza coraz dłuższe otwieranie się kolejnych stron aplikacji internetowej. W skrajnym przypadku aplikacja przestaje obsługiwać jakiekolwiek sesje, ponieważ nie posiada wystarczającej mocy obliczeniowej czy pamięci. W takim przypadku klikanie w poszczególne aktywne miejsca witryny WWW nie przynosi żadnego efektu, a w przeglądarce użytkownika pojawia się komunikat o braku odpowiedzi ze strony aplikacji internetowej czy serwisu WWW (w przeglądarce internetowej pojawia się informacja np. Błąd 500 - wewnętrzny błąd serwera).

Spis treści

Atak aplikacyjny w tunelu SSL

Istnieje także odmiana ataku aplikacyjnego, który realizowany jest z wykorzystaniem tunelu SSL.

Co to jest tunel SSL?

Tunel SSL to metoda wymiany danych, gdzie informacja przed wysłaniem podlega zaszyfrowaniu, a po przesłaniu jej Internetem do miejsca docelowego następuje odkodowanie zawartych w pakietach danych. W praktyce oznacza to tyle, że przesyłane dane na całej swojej drodze przez cyfrowy świat, nie są przesyłane w postaci jawnej tylko zaszyfrowanej. Tym samym przechwycenie takich danych nie pozwala na sprawdzenie jakiego typu informacja znajduje się w transferowanych pakietach. W przeglądarkach internetowych takie szyfrowane sesje internetowe można poznać po tym, że przed adresem internetowym pojawia się skrót: **https://**, zamiast http://

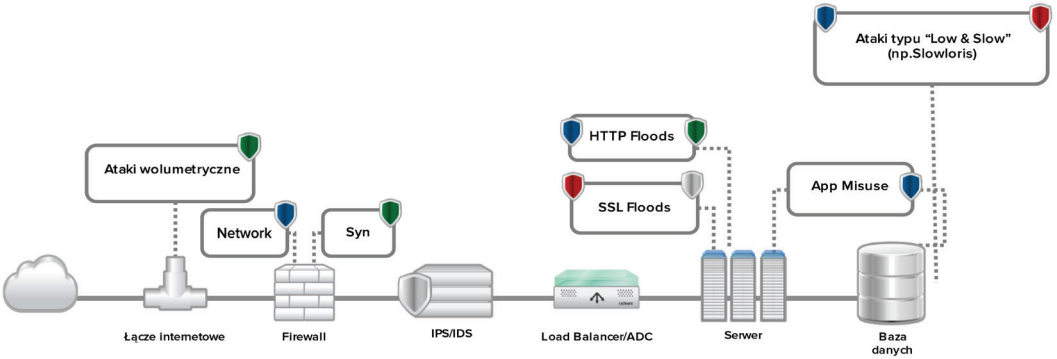
Takie bezpieczne przesyłanie informacji ma także negatywne konsekwencje, ponieważ może zostać wykorzystane do ataku hakerów na aplikację.

Pełna poufność przesyłanych danych wymaga, aby odkodowanie informacji następowało w aplikacji. Tym samym systemy ochronne (firewall) nie mają technicznej możliwości weryfikacji tego, co jest przesyłane i nie są w stanie zweryfikować czy tak szyfrowane sesje internetowe nie są atakiem hakerskim, np. DDoS. Obecnie bardzo szybko, z roku na rok, rośnie liczba tego typu ataków DDoS.

Spis treści

Co może być celem ataków DDoS?

Celem ataków DDoS może być parę miejsc w sieciach komputerowych. Poniżej schemat pokazujące najczęściej atakowane systemy.



Łącze internetowe

Do ataków na łącze internetowe wykorzystywane są wolumetryczne ataki DDoS (jest ich wiele rodzajów). Efektem skutecznego ataku DDoS jest przesłanie tak dużej ilości danych, które nie są w stanie być odebrane przez atakowane łącze internetowe. Przeciętne łącze internetowe w Polsce ma przepływność na poziomie 50-100Mb/s. Wolumetryczne ataki DDoS zaczynają się od 6-10Mb/s (te najmniejsze), przez 200-500Mb/s. Największy wykryty i odparty atak na świecie miał przepływność ponad 400Gb/s

Atak z początku 2016 r. miał podobno wielkości ponad 600Gb/s

Spis treści

Firewall

Coraz częściej celem ataku DDoS są urządzenia ochrony sieci komputerowej, powszechnie zwane **firewall**.

Systemy firewall mają za zadanie inspekcję każdej sesji internetowej, która jest zestawiana pomiędzy chronioną siecią a Internetem. Głównym zadaniem firewalli jest blokowanie niestandardowych prób zestawiania sesji czy innych zachowań, które świadczyć mogą o próbie włamania do chronionych zasobów.

Praktycznie tylko najdroższe rozwiązania firewall są przygotowane do mitygacji ataków DDoS (w tym ataków aplikacyjnych). Pozostałe systemy nie radzą sobie z atakiem DDoS. Dlaczego? Większość ataków DDoS to ataki na port 80, który jest wykorzystywany do przeglądania stron WWW. Z punktu widzenia firewall to otwarty port do komunikacji z Internetem, więc każda sesja internetowa która jest zestawiana z tym portem jest jedynie rejestrowana w specjalnym rejestrze. Problem w tym, że każdy firewall ma ograniczoną liczbę monitorowanych sesji, np. 100 tysięcy. Ataki DDoS powodują otwarcie miliona lub większej ilości sesji, co przyczynia się do przepełnienia rejestru i zaburza normalną pracę firewalla. W konsekwencji firewall nie pozwala na otwarcie kolejnej sesji internetowej, której nie jest w stanie monitorować, a tym samym rzeczywisty użytkownik chronionego serwisu internetowego, nie będzie mógł się połączyć z tym serwisem (np. stroną sklepu internetowego, czy portalem). Niektóre z firewalli posiadają specjalną funkcję, która oznacza się np. antiDDoS. Najczęściej ta funkcja nie ma nic wspólnego z ochroną przed atakami DDoS, a jedynie chroni samego firewalla przed przepełnieniem rejestru i zawieszeniem systemu ochrony.

Spis treści

IPS/IDS

Systemy wykrywania intruzów. To specjalne algorytmy analizy sesji internetowych, których zadaniem jest wykrywanie takich działań, które prowadzą do nieautoryzowanego wejścia do chronionych sieci czy zasobów informatycznych. Niektóre systemy IPS/IDS przestają poprawnie działać w skutek zbyt dużej ilości sesji internetowych, które podlegają analizie.

Load balancer/ADC

System równomiernego rozkładania obciążenia systemów informatycznych (pamięci, mocy procesora). Zadaniem takiego systemu jest przeciwdziałanie przeciążenia pojedynczego serwera. W przypadku źle dobranego lub skonfigurowanego Load balancera, może się okazać, że atak DDoS spowoduje utratę dostępności do aplikacji (pomimo tego, że posiada ona wolne zasoby informatyczne).

Serwery

To główny cel ataków hakerskich, w tym ataków DDoS. Celem jest wyczerpanie zasobów informatycznych przeznaczonych do realizacji funkcji serwisu internetowego czy aplikacji. Bardzo często ataki na aplikacje internetowe mają na celu dostanie się do bazy danych, która jest wykorzystywana do poprawnej pracy aplikacji internetowej.

Spis treści

Dlaczego ataki DDoS są tak trudne do wykrycia?

Obecne ataki DDoS są coraz bardziej wyrafinowane oraz od wielu lat spadają koszty ich przeprowadzania.

Jest parę kluczowych problemów z wykrywaniem ataków DDoS:

1. Atak DDoS najczęściej prowadzony jest na porty i z użyciem protokołów, które są używane przez przeglądarki internetowe, przez co bardzo trudno jest wyfiltrować jakieś charakterystyczne sesje internetowe lub ruch pakietów na konkretne porty.

2. Często atak DDoS prowadzony jest w postaci strumieni pakietów wysyłanych z tysięcy zawirusowanych komputerów, w tym przypadku użytkownicy tych komputerów (a nawet smartphone'ów) nie są świadomi tego, że uczestniczą w ataku DDoS. Tego typu „złośliwe oprogramowanie" używa komputera jako źródła zapytań internetowych do ataku na serwis internetowy ofiary.

3. Istnieje bardzo wiele metod zwielokrotnienia wielkości ruchu pakietów IP, jakie są wysyłane na łącze internetowe ofiary. Najbardziej skuteczne metody potrafią zwiększyć strumień IP nawet 4000-razy. Teoretycznie oznacza to, że wystarczy z jednego źródła wysłać strumień 100kb/s (dla porównania strumień wideo z serwisu YouTube potrzebuje ok. 13 000 kb/s), aby po zwielokrotnieniu, na łącze internetowe ofiary ataku DDoS trafił strumień danych 400 000kb/s (ok. 400Mb/s). W praktyce nie jest tak prosto wygenerować tak duży atak DDoS, choć nie wymaga on szczególnie dużych umiejętności hakerskich.

Spis treści

4. Ataki DDoS przeprowadzane z użyciem szyfrowania (tunele SSL) są szczególnie trudne do wykrycia i mitygacji (tłumienia), ponieważ wymagają bardzo wyrafinowanego rozwiązania technicznego.

5. Odparcie ataku wolumetrycznego DDoS jest bardzo trudne, ponieważ wysłanie olbrzymiej ilości pakietów danych na ograniczone łącze internetowe, zablokuje to łącze. Analiza przychodzącego ruchu IP i weryfikacja co to za pakiety i czy są otwarte porty dla takiego strumienia danych odbywa się dopiero na końcu tego łącza (u Klienta). Zatem odrzucenie niechcianych danych odbywa się na końcu ograniczonej „rurki internetowej", a to oznacza że dane najpierw blokują łącze, a dopiero potem systemy ochrony (np. firewall) dokonują analizy tego co udało się zmieścić do ograniczonego łącza internetowego. Co dzieje się z pakietami danych, które nie zmieściły się w danej chwili w paśmie łącza internetowego? **Są bezpowrotnie tracone.**

Spis treści

Kto atakuje DDoS'em i dlaczego?

Motywacji do przeprowadzania ataków DDoS jest wiele. To co istotne, nie trzeba posiadać specjalnych umiejętności hakerskich, aby taki atak DDoS przeprowadzić (o tym w następnym podrozdziale).

Grupę inicjatorów ataków DDoS można podzielić na parę kategorii:

Cyberwojownicy

To grupa osób, najczęściej działająca na zlecenie państw lub organizacji paramilitarnych, których celem jest dezorganizacja jakiegoś sektora danego państwa. Obecnie w ramach armii budowane są specjalne cyberjednostki, których zadaniem jest budowanie scenariuszy i narzędzi wykorzystywanych we współczesnych wojnach hybrydowych. Ataki DDoS stanowią jedno z ważnych narzędzi, którymi dysponują tego typu grupy.

Cyberprzestępcy

To grupa osób, których celem jest dokonywanie przestępstw komputerowych. Ataki DDoS stanowią najczęściej wstęp do ataków hakerskich, ponieważ atak DDoS bardzo mocno angażuje informatyków w firmach, przez co nie mają oni czasu na zajmowanie się monitorowaniem i reagowaniem na incydenty naruszenia bezpieczeństwa informatycznego w firmach. Atak DDoS z uwagi na swoją prostotę wygenerowania oraz olbrzymią trudność w odparciu przez ofiarę, jest coraz bardziej popularną metodą przygotowania do przeprowadzania włamań do sieci komputerowych. Ponadto bardzo popularną metodą jest **cyberszantaż**, polegający na wysłaniu do ofiary informacji z żądaniem zapłaceni okupu, w przeciwnym razie zostanie przeprowadzony atak DDoS na dany serwis internetowy (np. sklep internetowy). Praktycznie co miesiąc pojawiają się w sieci informacje o konkretnych grupach hakerskich, które w ten sposób wymuszają płacenie okupów. Szczególnie listopad 2015r. był bardzo obfity w działania z wykorzystaniem ataków DDoS na serwisy szyfrowanej poczty elektronicznej (więcej szczegółów na firmowym blogu DataSpace).

Haktiwiści

Grupa aktywistów, którzy ataki DDoS traktują jako formę protestu w Internecie. Blokowanie witryn internetowych rządowych instytucji odbywa się praktycznie każdego roku. Dotyczy to także serwisów internetowych korporacji czy innych przedsiębiorstw, który działanie wywołuje oburzenie społeczne. W Polsce najbardziej

Spis treści

znanymi były ataki DDoS przeprowadzone przez grupę **Anonymous** na strony internetowe policji, sejmu, Rady Ministrów, w czasie gdy trwały negocjacje nad przyjęciem ACTA.

Szpiegostwo

Istnieje szereg wyspecjalizowanych grup i firm zajmujących się szpiegostwem przemysłowym czy politycznym, których głównymi celem jest dotarcie do pilnie strzeżonych informacji. W ich przypadku ataki DDoS są wykorzystywane jak „zasłona dymna" do prób włamania się do pilnie strzeżonych sieci komputerowych.

Amatorzy

Z roku na rok rośnie liczba incydentów ataków DDoS, za którymi stoją osoby prywatne. Począwszy od nastolatków atakujących szkolne dzienniki elektroniczne, czy serwery gier, po sfrustrowanych byłych pracowników, którzy w ten sposób próbują odreagować na swoim byłym pracodawcy. Wcale nie trzeba być ekspertem informatycznym, aby przeprowadzić atak DDoS. Ale o tym w następnym rozdziale.

Spis treści

Ile kosztuje atak DDoS?

Pierwotnie ataki DoS (ataki wykonywane z jednego miejsca w Internecie), były dość drogie. Należało wynająć lub kupić serwer, zapłacić za prąd do tego serwera, wykupić odpowiednio duże łącze internetowe oraz uruchomić specjalną aplikację, która przeprowadzać będzie atak (wiele takich aplikacji jest dostępnych w modelu OpenSource, co daje możliwość kolejnym hakerom wykorzystania ich kodu do przygotowywania własnego, złośliwego oprogramowania). Tym samym do wykonania ataku wolumetrycznego DDoS o np. przepływności 1Gb/s należało posiadać łącze o takiej samej przepływności (takie łącze kosztuje parę tysięcy złotych każdego miesiąca). Jednak z czasem nastąpił rozwój technik ataków. Hakerzy nauczyli się wzmacniać atak, czyli nie potrzebowali już opłacać tak dużego łącza internetowego.

Obecnie do przeprowadzania ataków DDoS wykorzystywane są tak zwane **botnety**.

Co to takiego botnet?

Botnet to grupa zainfekowanych złośliwym oprogramowaniem (wirusem) komputerów. Twórca takiego złośliwego oprogramowania posiada specjalną aplikację, która pozwala mu kontrolować taką grupę zainfekowanych komputerów. W ten sposób, przy pomocy jednej aplikacji, haker jest w stanie uruchamiać zdalnie, na całej kontrolowanej grupie komputerów, różnego rodzaju aplikacje czy programy. Wszystko bez wiedzy właściciela komputera.

Największe wykryte sieci botnet liczyły miliony zainfekowanych złośliwym oprogramowaniem komputerów, rozsianych po całym świecie.

Wysyłanie informacji z takiej zorganizowanej grupy komputerów - gdzie każdy z nich zlokalizowany może być na różnych kontynentach - sprawia, że ochrona jest praktycznie niemożliwa. Próba ręcznego wytypowania źródeł ataku oraz podejmowanie działań mających ignorować ruch z tych komputerów - jest praktycznie niemożliwe.

Rozwój techniki ataków DDoS z wykorzystaniem botnet'ów drastycznie obniżył koszty przeprowadzenia ataków DDoS. Od tego momentu haker nie ponosi praktycznie żadnych kosztów związanych z atakiem:

- wykorzystuje moc obliczeniową zainfekowanego komputera,
- za prąd do komputera płaci jego właściciel (nieświadomy wirusa w swoim systemie),
- za łącze do Internetu płaci właściciel lub jego pracodawca.

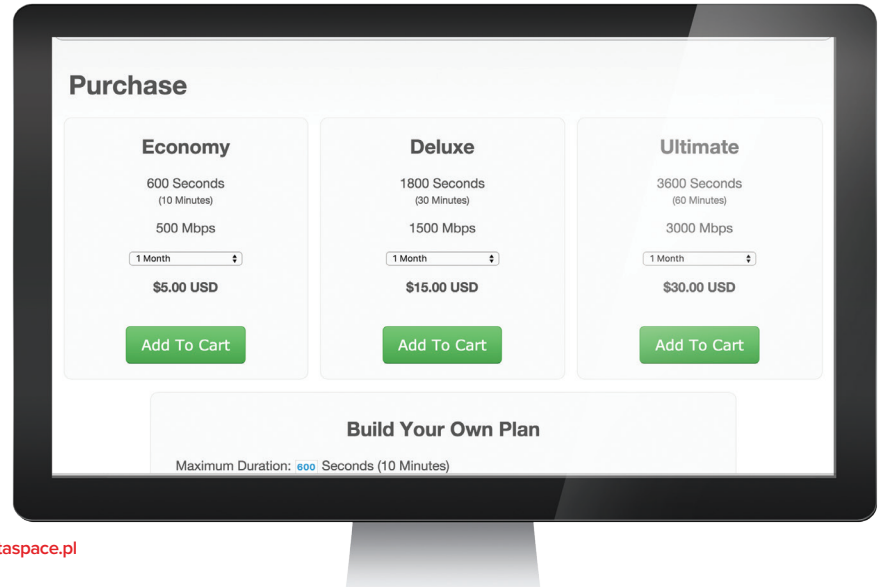
Spis treści

Jedyną pracą hakerów jest stworzenie wirusa wraz ze specjalnym programem do kontroli wszystkich zainfekowanych komputerów oraz opracowanie sposobu na rozpropagowanie wirusa w świecie (tutaj jest dziesiątki metod, począwszy od pirackiego oprogramowania, przez zainfekowane strony WWW, po rozsyłanie specjalnie spreparowanych wiadomości e-mail).

Ile kosztuje atak DDoS?

Obecnie w Internecie jest sporo serwisów, które pozwalają na realizację ataków DDoS na wskazany adres IP czy domenę. Część z nich sprawia wrażenie realnej usługi, która jest świadczona na zamówienie i odpowiedzialność zamawiającego – jako **usługa testów penetracyjnych** (np. dla potrzeb sprawdzenia przez administratora czy ich procedury i systemy są przygotowane do odparcia ataków DDoS).

Poniżej przykładowe ceny z jednej z takich stron oferujących stres testy. Zlecający atak może sobie ustawić parametry ataku, np. typ ataku DDoS, czas trwania, wielkość ataku DDoS, itd. Niektóre z systemów posiadają szereg funkcji dodatkowych, np. obchodzenie zabezpieczeń.



Spis treści

Mity związane z ochroną przed DDoS

Często administratorzy sieci komputerowych czy aplikacji internetowych, nie do końca rozumieją jak bardzo trudnym do obrony jest atak DDoS. W związku z tym pojawiło się szereg mitów i błędnych przekonań, że stosunkowo prosto i tanio można się zabezpieczyć przed atakami DDoS.

Mit #1. Wystarczy zwiększyć pasmo

To najpopularniejszy mit na temat ataków DDoS. Dla pokazania „błędu myślowego" wystarczy przytoczyć fakt, że w Polsce 17 lipca 2014r. zanotowana wielkość ataku DDoS na jeden z serwisów internetowych to 100 Gbps. Ile firm w Polsce jest w stanie zwiększyć swoje pasmo do 100 Gbps w przeciągu paru godzin? Odpowiedź na to pytanie powinna wystarczyć za wyjaśnienie, dlaczego odparcie ataku DDoS poprzez zwiększenie pasma to mit.

MIT #2. Chmura wchłonie każdy DDoS

Bardzo często można się spotkać z opinią: „Wystarczy zainstalować aplikację w chmurze i mamy problem DDoSów z głowy?"

Niekoniecznie. Istnieją dwa poważne problemy.

ZASOBY W CHMURZE SĄ OGRANICZONE

Twórcy aplikacji przewidują zapotrzebowanie na moc obliczeniową i pamięć z pewnym zapasem. Nigdy jednak te zasoby nie są nieograniczone. Warto wiedzieć, że istnieje wiele typów ataków DDoS, zwłaszcza typu *slow*, które mają właśnie na celu wyczerpanie tych zasobów. Wiąże się z tym drugi problem...

OCHRONA DDOS DATA CENTER NIE ZAWSZE CHRONI KLIENTÓW

Wiele centrów danych posiada aktywne systemy ochrony przed DDoS. Niestety w praktyce oznacza to zwykle ochronę tylko przed atakami wolumetrycznymi. Tylko nieliczne data center są zabezpieczone przed atakami aplikacyjnymi, a te – jak pokazują statystyki – stanowią prawie połowę ataków DDoS.

Ponadto data center dużo piszą o ochronie przed atakami DDoS, jednak nie definiują, w jaki sposób realizowana jest usługa dla Klienta. Bardzo często jest tak, że ochrona dotyczy całego ruchu IP, jaki trafia do data center – analiza dotyczy ataków skierowanych na wysycenie łącza data center, a nie zasobów konkretnego Klienta.

Nikt nie gwarantuje odparcia ataku DDoS dla aplikacji umieszczonej w chmurze, z zagwarantowaną przepływnością np. 100 Mbps.

Spis treści

Aby ochronić tak wąskie pasmo przed atakiem wolumetrycznym, system aktywnej analizy pakietów powinien mieć podzielony ruch IP wpływający do data center na małe podsieci przydzielone poszczególnym Klientom.

Dlaczego ma to takie znaczenie? Większość systemów wykrywających ataki DDoS bazuje na analizie próbek *netflow* – to coś w rodzaju skróconego opisu ruchu IP. Dzięki temu analizuje się nawet 500-razy mniej danych, jednak konsekwencją tego jest mniejsza skuteczność i spora bezwładność w wykrywaniu ataków DDoS.

Jeżeli analizie *netflow* poddaje się bardzo duży ruch IP, to do analizatora próbek *netflow* trafia co 1000-na próbka. W efekcie wykrywane są wyłącznie bardzo duże ataki wolumetryczne. Są operatorzy (także w Polsce), którzy posiadają ochronę przed DDoS, jednak jest ona skuteczna dla łączy o przepływności powyżej 10 Gbps.

Mniejsze ataki DDoS nie są wykrywane. Ile firm w Polsce posiada łącze 10 Gbps? Posadowienie aplikacji w chmurze nie oznacza więc braku kłopotów z DDoS. Warto dopytać firmę hostingową o szczegóły ochrony przed atakami.

MIT #3. Wystarczy przeczekać DDoS

Przeczekanie to najgorszy sposób reakcji, zwłaszcza dla systemów informatycznych, od których zależy sprawne działanie firmy czy instytucji.
Raporty wszystkich firm zajmujących się ochroną przed DDoS potwierdzają, że z roku na rok rośnie średni czas trwania tych ataków. Od 2014r. wielokrotnie wzrosła liczba ataków permanentnych, powstało nawet pojęcie ataku PDDoS, czyli permanentnego ataku DDoS, a to oznacza, że grupy hakerskie potrafią atakować serwisy internetowe praktycznie non-stop.

Czekanie to najgorszy sposób reagowania na DDoS!

Jeżeli grupa agresorów zorientuje się, że ofiara nie radzi sobie z odparciem ataku DDoS, to prawdopodobieństwo zapłaty okupu z dnia na dzień staje się coraz większe.

W końcu szefowie firmy „pękną" i stwierdzą „skoro nie możemy nic zrobić, to zapłaćmy ten okup".

Jakie koszty ataków DDoS mają hakerzy? Jedynym kosztem jest praca, jaką trzeba wykonać, aby zbudować botnet, jego wykorzystanie już potem praktycznie nic nie kosztuje. Dużo więcej do stracenia ma atakowana firma, począwszy od strat finansowych spowodowanych brakiem sprzedaży i odpływem Klientów, przez utratę reputacji, a skończywszy na poufnych danych (DDoS to często zasłona dymna, ułatwiająca przełamanie zabezpieczeń).

Spis treści

MIT #4. DDoS to przestępstwo, więc Policja mi pomoże

Źródłem tego mitu jest przeświadczenie, że skoro ktoś popełnia przestępstwo, to wystarczy zgłosić ten fakt do odpowiedniego organu ścigania i problem będzie rozwiązany.

Niestety w żadnym kraju rządowe służby nie przeciwdziałają atakom DDoS – od tego są komercyjne firmy. W przypadku służb mundurowych można co najwyżej liczyć na wsparcie w przypadku śledzenia przestępców, bazując na przesłanych mailem żądaniach okupu czy sposobie realizacji płatności.

Jeżeli nie jesteś instytucją państwową, to żadne służby zajmujące się cyberprzestępczością nie zajmą się twoim problemem. Niech do myślenia da fakt, że co roku wiele instytucji państwowych ogłasza przetargi na zapewnienie ochrony przed atakami DDoS.

Usługi te świadczą firmy prywatne, a nie rządowa agencja czy instytucja. Dotyczy to nie tylko Polski, ale wielu krajów Europy.

MIT #5. Reputacja jest dobra na wszystko

Często producenci systemów ochrony systemów komputerowych, tzw. firewalli, podpierają się wiedzą z różnego rodzaju **centrów reputacji** (własnych lub firm trzecich). W takich centrach gromadzone są informacje o adresach IP, z których przeprowadzone zostały ataki DDoS.

Metoda może i dobra dla ataków hakerskich, jednak w przypadku ataków DDoS, gdzie wykorzystywane są botnety - **centra reputacji tracą sens**.

Ten sam komputer może być źródłem ataku DDoS, jak również generować ruch rzeczywistego użytkownika. Wpisanie w centrum reputacyjnym takiego źródła jako generatora ataków DDoS nie przyniesie rozwiązania problemu, a czasami może przysporzyć sporo kłopotów firmie użytkującej taki firewall.

Wyobraźmy sobie, że na komputerze znajduje się złośliwe oprogramowanie (tzw. *malware*), generujący ataki DDoS. Nic o nim nie wiadomo, działa sobie w tle. W efekcie taki komputer dostaje się na listę reputacyjną z informacją, że jest źródłem ataku DDoS.

Gdy firewall odpyta taką listę, w przypadku sesji internetowej z tego komputera, ruch zostanie zablokowany!

Możliwa jest sytuacja, gdy próbujecie się zalogować do swojego konta w banku, a jego firewall uzna was za źródło ataku i uniemożliwi dostęp do aplikacji.

Spis treści

Warto bardzo doczytać i dopytać przedstawicieli producenta firewalla, przed czym tak naprawdę chroni ich system w zakresie ataków DDoS. Tylko bardzo drogie i zaawansowane systemy NGF rzeczywiście posiadają funkcje odpowiedniej analityki.

O ograniczeniach związanych z wielkością łącza internetowego, na którym zainstalowany jest firewall nawet nie wspominam – średniej wielkości atak wysyci pasmo i wszystkie funkcje anty DDoS firewalla będą bez znaczenia.

Jest jeszcze jeden problem z danymi zawartymi w centrum reputacyjnym – aktualizacja. Jeżeli dzisiaj najwięcej ataków DDoS generowanych jest z sieci botnet, czyli całej masy prywatnych komputerów, rozsianych po całym świecie. Do tego u większości operatorów internetowych, indywidualni klienci nie otrzymują stałego adresu IP – jest on przydzielany dynamicznie i praktycznie codziennie używamy innego adresu IP. To jaki jest sens sprawdzania adresu źródła ataku DDoS w takim centrum reputacyjnym, skoro źródło ataku codziennie będzie miało inny adres IP (czyli inny adres źródła)?

MIT #6. To mnie nie dotyczy, jestem za mały

To kolejny mit, który pokutuje wśród wielu administratorów sieci i aplikacji internetowych.

W praktyce za bardzo wieloma atakami hakerskimi stoją **automaty**. Specjalne skanery, które automatycznie przeczesują Internet, poszukując np. niezałatanej dziury w sieci LAN. Odnalezienie słabego miejsca w sieci uruchamia skrypty, których zadaniem jest dokonanie ataku, np. DDoS.

Bardzo rzadko hakerzy działają z precyzyjnie wyznaczonym celem, który obserwują, skanują, rozpoznają oraz wyczekują na odpowiedni moment do ataku.

Wielu hakerów to zawodowcy – łamanie zabezpieczeń to ich praca, dlatego nie marnują czasu na przypadkowe cele. Wielu z nich pisze skrypty, automatyzujące procesy, aby ataki realizowane były masowo i samoczynnie. W ten sposób automaty „podpowiadają" potencjalne cele, na których haker powinien skupić swoją uwagę.

Wykrycie słabego punktu w sieci uruchamia scenariusz ataku. W tym czasie nie tylko ofiara, ale także haker może spokojnie spać. Niedowiarkom proponuję zainstalować sobie na jakimś serwerze centralkę iPABX, np. Asteriska i pozostawić ją bez zabezpieczeń. Zapewne już po kilku dniach dojdzie do włamania i zmiany ustawień centrali.

To nie wielkość sieci czy systemu informatycznego może zdecydować o ataku, ale podatność na konkretny

Spis treści

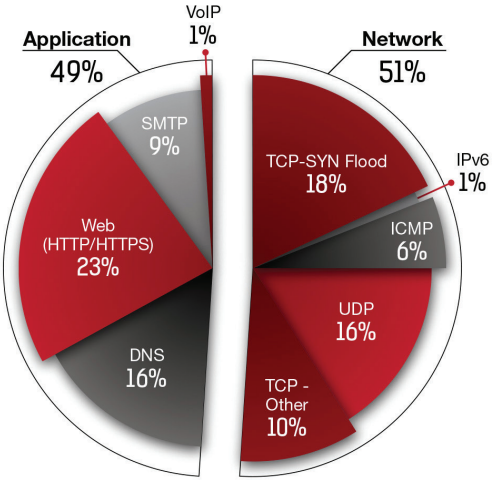
atak. Automat nie będzie oceniał czy dana firma jest duża, czy też mała. Wykona procedury i w raporcie do hakera przekaże efekty swojego działania. **Nie łudź się, że małemu nic nie zrobią!**

MIT #7: DDoS to atak sieciowy, najczęściej SYN FLOODS

Kolejny mit to przekonanie, że wśród ataków DDoS zdecydowaną większość stanowi jeden typ – **SYN Floods**. Kiedyś może tak było, ale te czasy dawno już minęły. Obecnie DDoSy to często wielowektorowe ataki zarówno sieciowe, jak i aplikacyjne. Poniższy wykres pokazuje rozkład najważniejszych typów ataków w 2014r.

Rzeczywiście SYN Floods jest popularny, ale to tylko 18% wszystkich DDoSów. Co istotne, popularność tego rodzaju ataku spada z roku na rok – w 2012r. stanowił on ponad 35% całości.

Powyższe statystyki potwierdzają także dane od providerów, którzy oferują usługi antyDDoS – ataki aplikacyjne są równie popularne, jak sieciowe.



Rysunek2. Statystyczny rozkład rodzajów ataków DDoS (źródło: RADWARE)

Spis treści

Cześć II.
Jak się obronić przed atakiem DDoS?

Obrona przed atakami DDoS wymaga dokładnej analizy konkretnego przypadku. W dalszej części przedstawione zostaną możliwe scenariusze, które pozwolą na ochronę przed atakami DDoS.

Łącze internetowe z ochroną DDoS

To jeden z wariantów ochrony, którą oferują operatorzy ISP. Usługa polega na dostarczeniu łącza internetowego, które pozwala na uruchomienie specjalnej usługi ochrony przed atakami DDoS.

Biorąc pod uwagę takie rozwiązanie warto wiedzieć, że:

1. Musimy zestawić łącze internetowe z siecią tego konkretnego operatora ISP (jeżeli nie mamy takiego łącza obecnie, to musi zostać ono zestawione czy zbudowane – a to oznacza wypowiedzenie umowy z obecnym operatorem ISP, zmianę adresów IP, czasami zmianę procedur eskalowania problemów, itd.),

2. Ochrona realizowana przez operatorów ISP najczęściej bazuje na analizie próbek *netflow*, czyli na analizie skrótowej informacji o ruchu IP danego łącza. W zależności jak dużo takich próbek *netflow* jest analizowanych, tak szybko może nastąpić wykrycie ataku DDoS. Im mniej próbej jest analizowanych, tym dłużej trwa proces wykrycia ataku DDoS. Ponadto analiza próbek *netflow* pozwala na wykrywanie ataków wolumetrycznych, natomiast nie radzi sobie z wykrywaniem ataków aplikacyjnych.

3. Usługa ochrony realizowana przez operatora ISP **nie jest w pełni automatyczna**. Najczęściej jest *półautomatyczna*, co oznacza że automatycznie wykrywana jest anomalia na ruchu IP danego łącza, jednak decyzja o skierowaniu tego ruchu do szczegółowej analizy i mitygacji ataku DDoS wymaga już reakcji administratora po stronie operatora. To operator wstępnie musi

Spis treści

przeanalizować anomalię, aby stwierdzić czy to jest początek ataku DDoS. W zależności od operatora, średnio taka czynność zajmuje od 15 do 30 minut. To wystarczająca ilość czasu, aby atak DDoS wysycił łącze internetowe, odciął serwis internetowy czy sieć komputerową, a hakerzy mieli dość czasu, aby przedostać się do chronionych zasobów i zainstalować tam złośliwe oprogramowanie, które pozwoli w niedalekiej przyszłości dostać się do chronionego systemu z pominięciem systemów zabezpieczeń (np. poprzez zestawienie szyfrowanego tunelu SSL).

To tylko podstawowe fakty, o których warto wiedzieć wybierając system ochrony przed atakami DDoS.
(więcej można informacji można znaleźć na firmowym blogu Data Space)

www.dataspace.pl

Spis treści

Scrubbing Center - co to takiego i jakie są scenariusze ochrony

Dużo praktyczniejszą metodą ochrony przed atakami DDoS jest wykorzystanie usługi ochrony z użyciem Scrubbing Center.

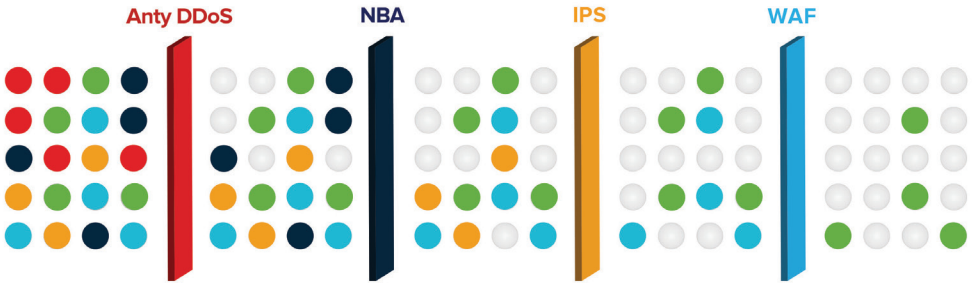
Co to jest Scrubbing Center?

Scrubbing Center to specjalnie zbudowane centrum analizy ruchu IP, gdzie następuje pełny monitoring pakietów danych, analiza anomalii oraz mitygacja wykrytych ataków DDoS lub prób włamania. Usługa ochrony przed atakami DDoS, w których wykorzystuje się Scrubbing Center może być realizowana na różne sposoby (więcej szczegółów w dalszej części).

Jak działa Scrubbing Center?

Analizowany ruch pakietów IP podlega weryfikacji i analizie na różnych poziomach. Rysunek na następnej stronie prezentuje poszczególne fazy analizy.

Spis treści



Rysunek 3. Fazy analizy ruchu IP w Scrubbing Center

Poniżej krótki opis poszczególnych faz analizy:

Anty DDoS

Analiza polegająca na wykryciu w ruchu IP takich pakietów, które nie są adresowane do aplikacji, serwisu, sieci komputerowej, która podlega ochronie. Na tym poziomie następuje odrzucenie wszelkich pakietów, które są niepoprawne (niezgodne ze standardem danego protokołu).

NBA

(ang. Network Behavioral Analysis) – analiza behawioralna źródeł danych; to bardzo zaawansowana technika analizy, wykorzystująca szereg algorytmów sztucznej inteligencji, której zadaniem jest analiza zachowań każdego ze źródeł ruchu IP, wykrycie wszelkich anomalii czy „dziwnych zachowań", świadczących o sztucznym pochodzeniu danego ruchu IP.

IPS

(z ang. Intrusion Prevention System) – zadaniem tego system jest wykrywanej wszelkiej aktywności, która świadczyłaby o próbach włamania się do chronionego serwisu czy sieci komputerowej. To w tym systemie następuje wykrycie aktywności hakerów oraz monitorowanie pola „DANE", w którym przesyłane jest złośliwe oprogramowanie (systemy blokuje transfer złośliwego oprogramowania).

WAF

(z ang. Web Application Firewall) – dedykowany system, którego zadaniem jest monitorowanie zachowań użytkowników w konkretnym serwisie internetowym lub aplikacji internetowej. Celem jest weryfikacja każdej aktywności użytkownika, włącznie z wprowadzaniem wszelkich danych w formularzach serwisu internetowego. Ochrona aplikacji jest szczególnie trudna, ponieważ pisane aplikacje nie

Spis treści

posiadają żadnego standardowego scenariusza budowy aplikacji, aby była ona bezpieczna. Większość firm piszących oprogramowanie nie posiada kompetencji do sprawdzania wrażliwości stworzonego oprogramowania na ataki hakerskie, w tym na ataki DDoS. WAF jest narzędziem, które „uczy się" aplikacji i potrafi wykrywać zachowania użytkowników, które mogą być groźna dla stabilności pracy aplikacji lub są próbą włamania się do danych aplikacji.

Jak ruch IP trafia do Scrubbing Center?

Rozpatrując Scrubbing Center w scenariuszu ochrony, należy wiedzieć jak technicznie kierować można ruch IP do takiego centrum analizy pakietów. Są dwie podstawowe metody przekierowania ruchu IP do Scrubbing Center:

METODA I (DOMENOWA)

Każdy serwis internetowy (strona WWW, sklep internetowy, itp.) skojarzony jest z konkretną domeną (np. www.fajnysklep.pl). Każda domena musi być skojarzona z konkretnym adresem IP, na który będą kierowane wszystkie zapytania i pakiety IP związane z serwisem powiązanym z daną domeną.

Aby skierować ruch IP do Scrubbing Center, należy w serwerze DNS dokonać zmiany obecnego adresu IP na adres IP wskazany przez administratora Scrubbing Center.

Informacja o nowym adresie IP w przeciągu parunastu godzin zostanie rozdystrybuowana do wszystkich serwerów DNS, na całym świecie.

Od tego momentu każdy użytkownik, który wpisze w przeglądarce tę domenę (np. www.fajnysklep.pl) sprawi, że przeglądarka internetowa będzie wysyłała wszystkie komunikaty na adres IP Scrubbing Center. Jak odfiltrowanie pakiety trafiają do serwisu opisujemy poniżej.

METODA II (ADRESACJA)

W przypadku ochrony konkretnych adresów IP (np. sieci komputerowych) Scrubbing Center ustawiane jest w systemach chronionej sieci jako Proxy, czyli Scrubbing Center staje się pośrednikiem w przesyłanym ruchu IP (w obie strony) konkretnej sieci komputerowej.

Spis treści

METODA III (BGP REDIRECTING)

W przypadku Klientów, którzy posiadają własne adresy IP oraz punkt AS (z ang. *Autonomous System*) jest możliwość dynamicznego zarządzania trasami pakietów IP. Ponadto Klient musi posiadać systemy sieciowe wspierające protokół BGP, który służy do dynamicznego trasowania (ang. *routing policy*). Przy spełnieniu powyższych warunków możliwe jest kierowanie ruchu IP konkretnej puli adresów IP (minimalna podsieć /24) do Scrubbing Center. To bardzo szybka metoda zarządzania rozpływem ruchu IP, którą może wykorzystać administrator danego serwisu internetowego. Ta metoda wymaga spełnienia paru warunków dodatkowych oraz uzgodnień administratorów Scrubbing Center jak również administratora chronionego serwisu/sieci.

Jak ruch wychodzi ze Scrubbing Center?

Po analizie i mitygacji ataków, ruch IP ze Scrubbing Center może być przesłany dalej na 2 sposoby:

SPOSÓB I (REVERSEPROXY)

Scrubbing Center może pełnić funkcję ReverseProxy dla aplikacji internetowej. Oznacza to, że w Internecie widoczny będzie adres IP Scrubbing Center, a ruch IP ze Scrubbing Center trafi na wskazany adres IP, na którym działa rzeczywiście chroniona aplikacja internetowa. Scrubbing Center jest w stanie przekazywać wszelkie istotne dla aplikacji internetowej informacje, np. o źródle ruchu IP (informacja wykorzystywana często do analizy statystycznej ruchu w serwisach internetowych).

SPOSÓB II (TUNEL)

Drugim sposobem przesłania ruchu IP ze Scrubbing Center do chronionego serwisu internetowego lub sieci komputerowej jest wykorzystanie tunelu GRE. W tym przypadku zestawiany jest tunel GRE, do którego wprowadzany jest odfiltrowany ruch IP.

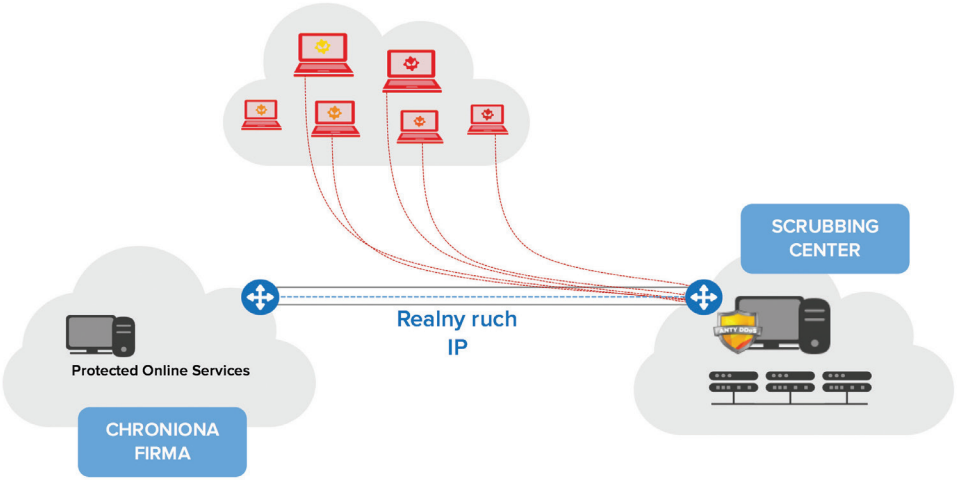
Spis treści

Scenariusze ochrony ze Scrubbing Center

Scrubbing Center może być wykorzystane do realizacji usługi ochrony przed atakami DDoS na parę sposobów. Poniżej krótka charakterystyka każdego z podstawowych scenariuszy.

OCHRONA PERMANENT

W przypadku scenariusza Permanent ruch IP kierowany jest od razu do Scrubbing Center, gdzie następuje jego analiza i mitygacja każdego wykrytego ataku lub prób włamania. Ten sposób ochrony jest praktykowany w przypadku, gdy chroniona jest aplikacja internetowa o niedużym ruchu IP (do 100Mb/s). Ograniczenie wynika wyłącznie z ekonomii rozwiązania, a nie możliwości technicznych.



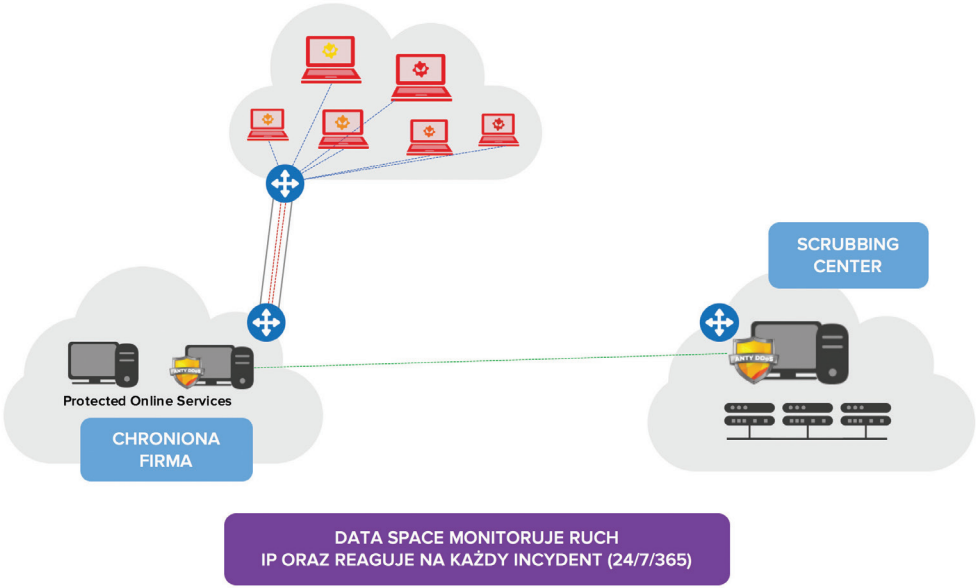
Rysunek 4. Schemat drogi pakietów dla ochrony typu Permanent.

Spis treści

OCHRONA HYBRYDOWA

Rozwiązanie hybrydowe przeznaczone jest dla najbardziej wymagających Klientów, którzy chcą mieć maksymalną kontrolę nad ruchem IP oraz pełną ochronę swojej aplikacji internetowej czy serwisu.

W rozwiązaniu tym wykorzystuje się specjalny moduł systemu ochrony, który zainstalowany jest bezpośrednio na chronionym łączu. Moduł systemu ochrony komunikuje się z centralnym systemem zarządzania Scrubbing Center (przesyła raporty i informacje o wykrytych atakach, nie tylko DDoS).



Rysunek 5. Rozpływ ruchu IP i informacji o atakach w przypadku ochrony hybrydowej (stan bez ataku wolumetrycznego DDoS).

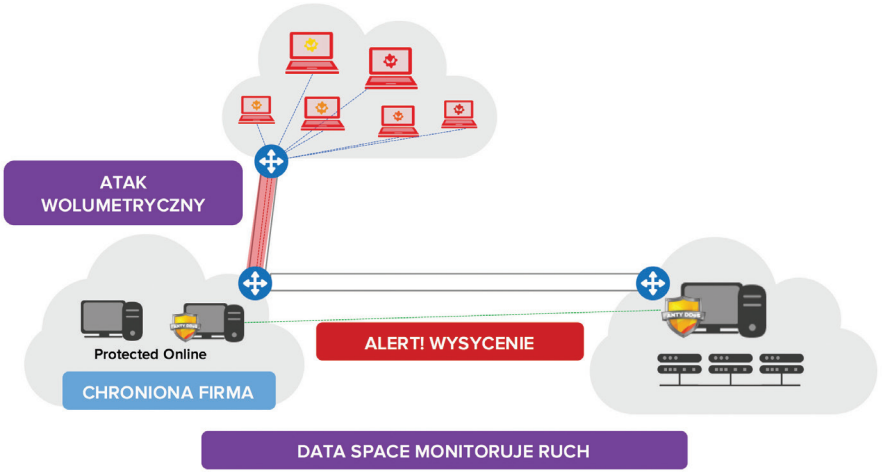
Spis treści

Przy takiej konfiguracji i rozpływie ruchu IP, moduł systemu ochrony zainstalowany bezpośrednio na łączu, chroni przed wszystkimi atakami na aplikacje internetowe (nie tylko przez atakami DDoS, ale także posiada funkcję IDS, NBA oraz może posiadać również WAF). Wykrywane i mitygowane są wszystkie ataki (włączając w to ataki aplikacyjne DDoS), ponieważ moduł systemu ochrony posiada identyczne funkcje i inteligencję jak system centralny w Scrubbing Center. Różni się tylko wydajnością.

Jednak sam moduł ochrony nie jest w stanie mitygować ataków wolumetrycznych DDoS, które wysycają łącze internetowe. Co można zrobić, aby poradzić sobie w przypadku ataku wolumetrycznego DDoS, który wysyci możliwości łącza internetowego?

W takim przypadku do akcji wkracza Scrubbing Center.

Po pierwsze centralny system zarządzania posiada pełną wiedzę o wykrytych atakach na chronione łącze, ponadto gwałtowny przyrost ruchu IP lub osiągnięcie założonego wysycenia łącza (np. przekroczenie poziomu 75% wydajności), sprawia że administratorzy Scrubbing Center zostają powiadomieni alertem. W taki przypadku uruchamiany jest proces przekierowania ruchu IP do Scrubbing Center (możliwe scenariusze opisane zostały powyżej).

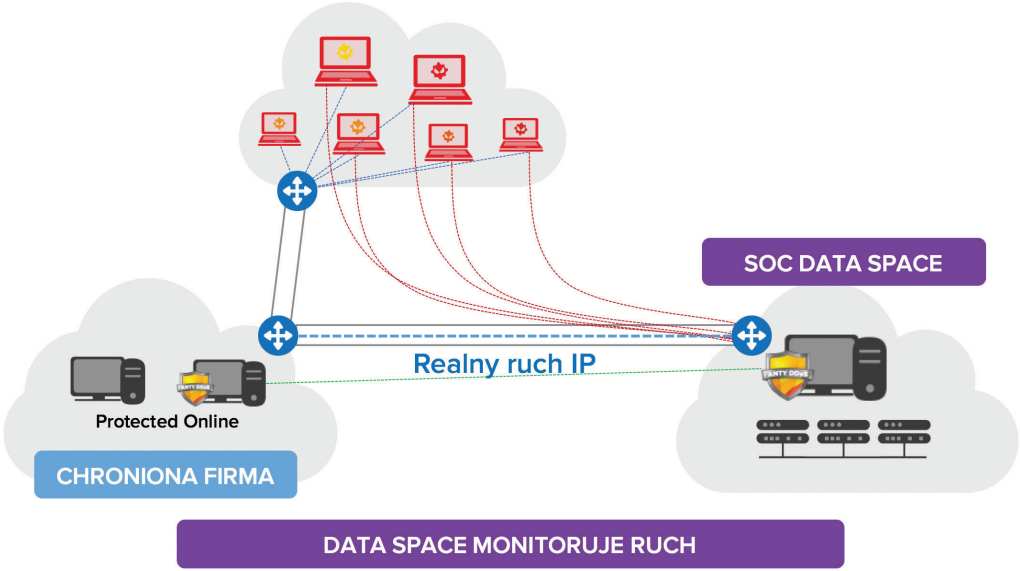


Rysunek 6. Rozpływ informacji w przypadku ataku wolumetrycznego.

Spis treści

W zależności od metody, w przeciągu parunastu minut cały ruch IP zamiast trafiać na chronione łącze internetowe, trafia na łącza wykorzystywane przez Scrubbing Center (tutaj wykorzystywane są łącza o przepływności nx10Gb/s). Centralny system zarządzania ma pełną charakterystykę wykrytego ataku, ponieważ moduł systemu ochrony na bieżąco przesyłał wszystkie informacje. Tym samym nie ma żadnej zwłoki w tłumieniu wykrytego ataku, ponieważ jego charakterystyka jest już znana, a pojawienie się kolejnych, nowych wektorów ataku powoduje automatyczne uruchomienie procesów obronnych w systemie Scrubbing Center.

Odfiltrowany ruch IP przesyłany jest chronionego systemu w jeden ze sposobów opisany powyżej.



Rysunek 7. Rozpływ ruchu po przekierowaniu ruchu IP do Scrubbing Center.

Spis treści

OCHRONA SATURATE

W przypadku ochrony **Saturate** monitorowane jest chronione łącze, jednak alert pojawia się wyłącznie w przypadku ataków wolumetrycznych DDoS (patrz Rysunek. 8). Ochrona przed pozostałymi typami ataków odbywa się po stronie Klienta i wykorzystuje on do tego swoje własne systemy ochronne.

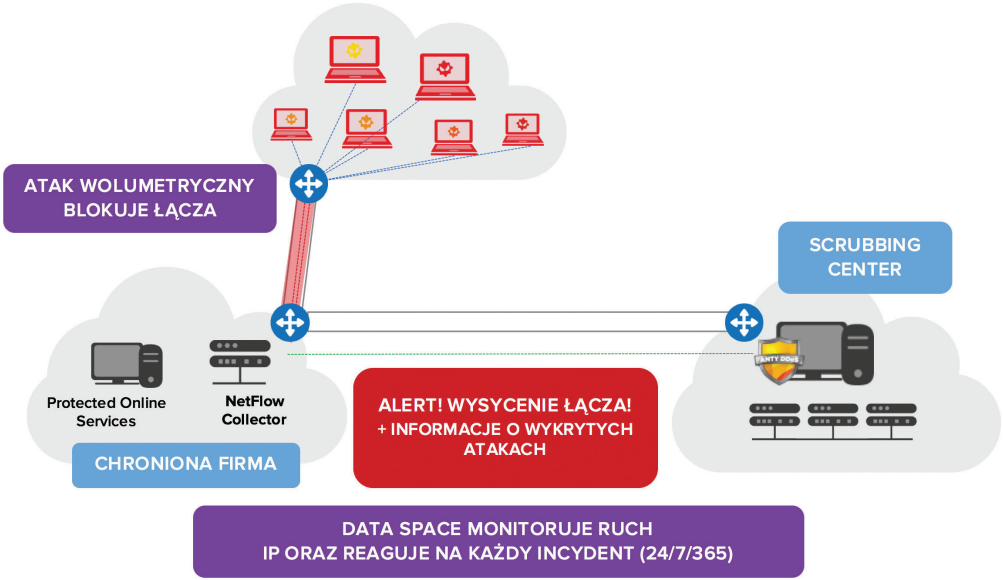
W tym modelu ochrony wykorzystywany jest jedynie system do monitorowania ruchu IP na chronionym łączu. System monitorowania ruchu IP wykrywa wyłącznie wolumetryczne DDoS, a analizie podlegają próbki netflow generowane przez urządzenie sieciowe Klienta. System analizujący próbki netflow jest zintegrowany z centralnym systemem zarządzania w Scrubbing Center i w przypadku wykrycia wolumetrycznych ataków DDoS przesyła sygnaturę każdego takiego ataku do Scrubbing Center. Dzięki temu mechanizmowi baza wiedzy o bieżących atakach na chronionych łączach jest aktualna i systemy obronne w Scrubbing Center są gotowe do natychmiastowego zareagowania, gdy ruch IP trafi do Scrubbing Center.

W ochronie Saturate po przesłaniu alertu do administratorów Scrubbing Center następuje procedura przekierowania ruchu IP do Scrubbing Center (jedna z metod opisana powyżej).

W momencie, gdy ruch IP trafi do Scrubbing Center – system obronny ma pełną wiedzę o wykrytym ataku wolumetryczym i natychmiast rozpoczyna proces filtrowania ruchu IP. Jednocześnie następuje analiza ruchu IP pod względem innego typu ataków i w przypadku wykrycia kolejnych wektorów ataków DDoS, uruchamiane są procesy obronne.

Odfiltrowany ruch IP przesyłany jest do chronionej aplikacji czy serwisu w sposób opisany powyżej.

Spis treści



Rysunek 8. Rozpływ ruchu IP i informacji w przypadku ochrony Saturate i wykrycia ataku wolumetrycznego DDoS.

Spis treści

OCHRONA 2READY

Pewna grupa Klientów posiada zarówno kompetencje jak i własne systemy ochrony przed atakami hakerskimi. Jedynym typem ataku, z którym nie są sobie w stanie poradzić są ataki wolumetryczne DDoS.

W takich przypadkach najlepiej sprawdza się ochrona **2Ready**. Polega on na tym, że Scrubbing Center posiada w pełni uzgodnioną procedurę informowania przez Klienta Scrubbing Center, o problemach z atakiem wolumetrycznymi.

Scrubbing Center jest w pełni skonfigurowane i przygotowane na przyjęcie ruchu IP atakowanego Klienta. W momencie gdy ruch IP trafi do Scrubbing Center rozpoczyna się proces analizy i wykrywania ataków w strumieniu pakietów Klienta. System Scrubbing Center w przeciągu parudziesięciu sekund wykrywa wszelkie ataki DDoS i uruchamia proces obronne. Odfiltrowany ruch IP kierowany jest do chronionej aplikacji Klienta w uzgodniony wcześniej sposób.

W tym modelu ochrony system ochronny Scrubbing Center nie posiada żadnej wiedzy o ataku, dopiero trafiający ruch IP uruchamia proces wykrywania i mitygacji ataków DDoS.

Ochrona 2Ready jest usługą dostępną w trybie całodobowym (24/7). Jednak, aby z niej skorzystać należy wcześniej uzgodnić wszystkie parametry techniczne oraz procedury powiadamiania, aby reakcja była maksymalnie szybka.

Spis treści

Zalety rozwiązania ze Scrubbing Center

Stosowanie w scenariuszu ochrony przed atakami DDoS możliwości Scrubbing Center posiada następujące zalety.

Nie musisz zmieniać operatora

Jeżeli obecny operator ISP nie posiada usługi ochrony przed atakami DDoS lub usługa jest bardzo droga, albo też jakość ochrony jest niewystarczająca, to nie musisz podpisywać nowej umowy z nowym operatorem ISP. Rozwiązanie ze Scrubbing Center jest niezależne od operatora ISP. Usługa dostępu do Internetu może być realizowana przez dowolnego operatora internetowego.

Nie musisz zmieniać adresów IP

Uruchomienie ochrony przed atakami DDoS, z wykorzystaniem Scrubbing Center, nie wymaga zmiany adresów IP (dzieje się tak zawsze, gdy zmienia się operatora ISP).

Nie musisz kupować nowego systemu ochrony

W przypadku rozwiązania ze Scrubbing Center nie musisz kupować nowych systemów ochrony. Jeżeli posiadasz już firewalle, bądź inne systemy ochrony przed atakami hakerskimi to Scrubbing Center nie wymaga modyfikacji żadnego z nich. Scrubbing Center w takim wypadku stanowi jedynie uzupełnienie obecnych możliwości obrony i stanowić może drugą linię wsparcia. Dotyczy to zwłaszcza ataków wolumetrycznych lub wielowektorowych ataków na aplikację internetową (wiele firewalli nie radzi sobie z wielowektorowymi atakami, ponieważ ma zbyt małe możliwości obliczeniowe lub zbyt małą inteligencję, potrafiącą korelować wiele zdarzeń jednocześnie).

Nie musisz ciągle szkolić się z zakresu bezpieczeństwa

Systemy ochrony informatycznej nie należą do systemów, które wystarczy tylko włączyć. Wymagana jest ciągłą analiza i monitorowanie stanu ochrony, abym mieć maksymalną pewność, ze systemy działają poprawnie oraz że ich algorytmy i bazy danych są na bieżąco aktualizowane. Ponadto każdy administrator systemów ochrony musi regularnie doszkalać się z nowych form ataków, aby znać nowopowstałe scenariusze ataków hakerskich.

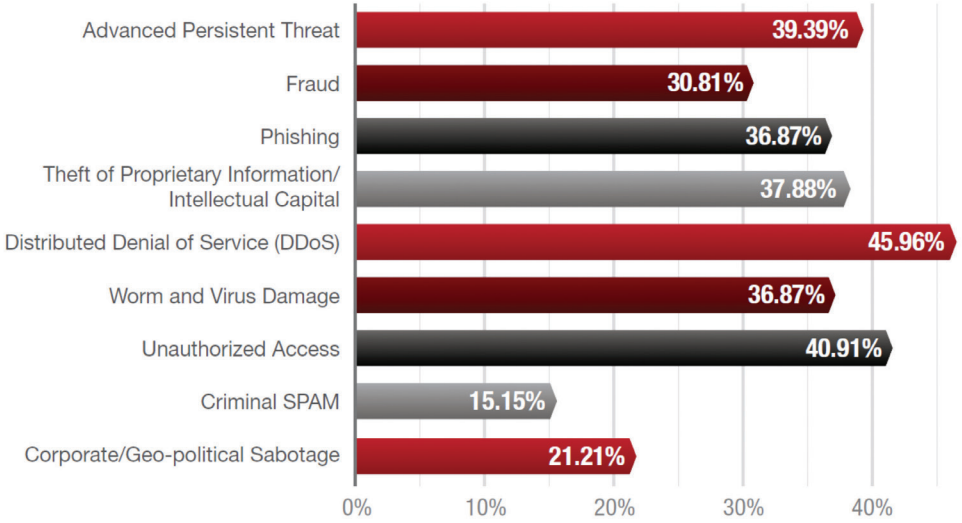
Spis treści

Odrobina statystyki z kraju i ze świata

Poniżej informacje z raportów firm specjalizujących się w ochronie przed atakami DDoS. Przedstawione wykresy odpowiadają na szereg pytań, które często zadają administratorzy aplikacji internetowych czy łączy internetowych.

Czy ataki DDoS to problem?

Poniższy wykres pokazuje procentowy udział ataków DDoS w różnego rodzaju atakach hakerów.



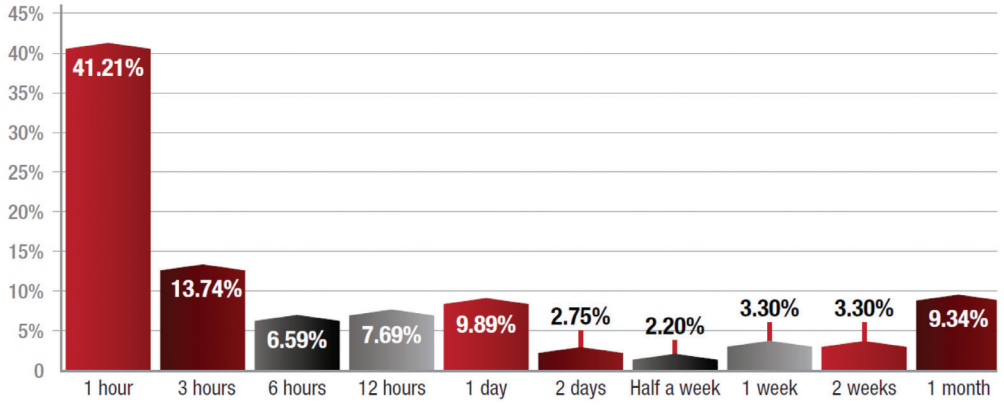
Wykres 1. Procentowy udział różnych typów ataków (źródło: RADWARE, raport 2014-2015).

Statystyki nie pozostawiają złudzeń, ataki DDoS to lider wśród metod stosowanych przez hakerów.

Spis treści

Jaka jest średnia długość ataków DDoS?

Ataki DDoS nie mają stałej długości. Czas trwania ataku uzależniony jest od wielu rzeczy i dobierany przez atakującego. Poniżej wykres pokazujący jak statystycznie wyglądają czasy ataków DDoS.



Wykres 2. Procentowy rozkład czasów trwania ataków DDoS (źródło: Radware, raport za 2014-2015).

Porównanie wyników rok do roku, ujawnia rosnący trend wydłużania czasu trwania ataków DDoS. Ponadto w przypadku wielowektorowych ataków stosowana jest cykliczność, która objawia się tym, że ataki są regularnie powtarzane w pewnych odstępach czasu, np. co parę godzin lub co parę dni. W ostatnich latach pojawiło się pojęcie ciągłego ataku DDoS, które określa się skrótem PDDoS (z ang. Permanent DDoS).

Spis treści

Kto w Polsce był atakowany DDoS'em?

Firmy i instytucje nie chwalą się medialnie problemami związanymi z atakami DDoS. Wszystkie polskie banki doświadczają praktycznie każdego miesiąca próbnych ataków DDoS. Ponadto wiele firm, które stały się ofiarami ataków DDoS, nie chwali się tym faktem szczególnie, wychodząc z założenia, że w ten sposób chronią swój wizerunek.

CERT Polska potwierdza występowanie ataków DDoS na ważne instytucje w naszym kraju. W raporcie z 2014 roku można przeczytać:

„W 2014 warte uwagi były ataki wymierzone w witrynę Prezydenta RP i w witryny Giełdy Papierów Wartościowych".

Ponadto w raporcie informuje się, że w marcu 2014r. pojawiła się nowa metoda ataków DDoS wykorzystująca popularnego CMS, jakim jest system Wordpress.

Rządowy CERT.GOV.PL również w swoich raportach sporo miejsca poświęca atakom DDoS. W 2014r. CERT.GOV.PL odnotował co najmniej 20 poważniejszych incydentów związanych z atakami DDoS. Największe konsekwencje miał atak DDoS na GPW, gdzie hakerom udało się przedostać przez systemy ochronne i uzyskać dostęp do poufnych informacji.

Należy przy tym zauważyć, że świadomość zagrożenia tego typu atakami w Polsce jest wciąż bardzo mała. Ponadto wiele ataków aplikacyjnych DDoS traktowanych jako „dziwne zachowanie aplikacji, które z czasem mija". Wynika to między innym z braku profesjonalnych narzędzi do identyfikowania takich form ataków hakerów.

W naszym Scrubbing Center praktycznie codziennie rejestrujemy ataki DDoS na serwisy naszych Klientów. Praktycznie nie ma godziny, aby system nie zidentyfikował ataku. Najwięcej jest ataków o małym natężeniu o przepływności 10-20Mbps. Jednak co jakiś czas pojawiają się ataki na poziomie 50-100Mbps, a nawet 1-2Gbps.

KNF ostrzega i wymaga

Urząd Kontroli i Nadzoru Finansowego regularnie ostrzega przed atakami DDoS na instytucje finansowe. Jednocześnie wydał zarządzenie, które zobowiązuje każdy podmiot finansowy w Polsce do przygotowania procedury postępowania na wypadek ataku DDoS. Każda instytucja w Polsce do końca 2016r. musi być przygotowana na wystąpienie ataków DDoS.

Spis treści

Web Application Firewall

Web Application Firewall to bardzo specyficzny system do ochrony aplikacji internetowej. Rolą takiego systemu jest monitorowanie zachowań użytkowników i reagowanie na wszelkiego rodzaju próby destabilizacji samej aplikacji lub próby pokonania zabezpieczeń.

Czym powinien charakteryzować się porządny Web Application Firewall?

1. **Transparentność** – monitorowanie zachowań użytkowników nie powinno wpływać na działanie samej aplikacji. Dotyczy to szczególnie aplikacji, od których wymaga się bardzo szybkiej reakcji na zachowania użytkownika, np. aplikacje bankowe.

Selektywna analiza ruchu IP – monitorowanie ruchu IP trafiającego do aplikacji internetowej powinno odbywać się bardzo szczegółowo, z uwzględnieniem poszczególnych protokołów, strumieni danych, itd. Ponadto WAF powinien potrafić analizować ruch zakodowany w tunelach SSL. Solidny WAF jest w stanie monitorować poprawność wszystkich procesów związanych z płatnościami on-line (PCI DSS, itd.).

2. **Prostota** – rozwiązanie WAF powinno być proste w implementacji, najlepiej gdy jest to pojedyncze urządzenie, które dokonuje analizy. Rozwiązania, które wymagają instalowania dodatkowych sond programowych (mikroprogramów, umieszczanych w kodzie chronionej aplikacji internetowej) jedynie komplikują rozwiązanie, a także mogą doprowadzić do niestabilnej pracy systemów.

3. **Skalowalność** – system WAF powinien być przygotowany na prostą i szybką rozbudowę. Jeżeli popularność aplikacji internetowej będzie rosnąć, to trudno sobie wyobrazić wyłączenie jej na czas przygotowania nowego WAF'a.

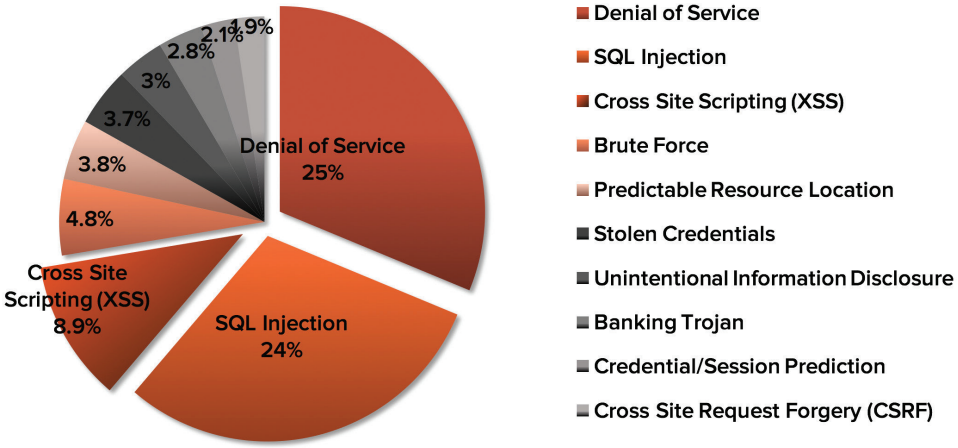
4. **Redukcja opóźnienia** – system monitorujący nie powinien wpływać znacząco na czas obsługi poszczególnych sesji internetowych. Najlepsze rozwiązania potrafią pracować na kopii ruchu IP, tym samym nie dodają żadnego opóźnienia w monitorowanym strumieniu danych.

5. **Wysoka dostępność** – w przypadku aplikacji internetowych, które wymagają gwarancji ciągłości pracy, takie same wymagania stają przed systemem WAF. Dobry system WAF powinien pozwalać na przygotowanie takiego trybu swojej pracy, aby zapewnić HA (*High Availability*).

Spis treści

Czy warto stosować WAF?

Statystyki dotyczące metod ataków hakerów nie pozostawiają złudzeń.



Wykres 1. Źródło: Web Hacking Incident Database (WHID), Feb. 2013

Ataki DDoS królują, jednak na kolejnych miejscach są ataki skierowane na warstwę aplikacji. Począwszy od prób wstrzyknięcia SQL, próby złamania haseł, po wirusy skierowane na transakcje bankowe. Każda z powyższych prób włamania skierowana jest na działania na aplikacji internetowej.

Skontaktuj się z nami

Masz pytania? Jesteśmy do Twojej dyspozycji.

Krzysztof Surgut
CEO

+48 510 219 468
krzysztof.surgut@dataspace.pl

Michał Gąszczyk
Business Development Director

+48 505 840 878
michal.gaszczyk@dataspace.pl