KASPERSKY lab

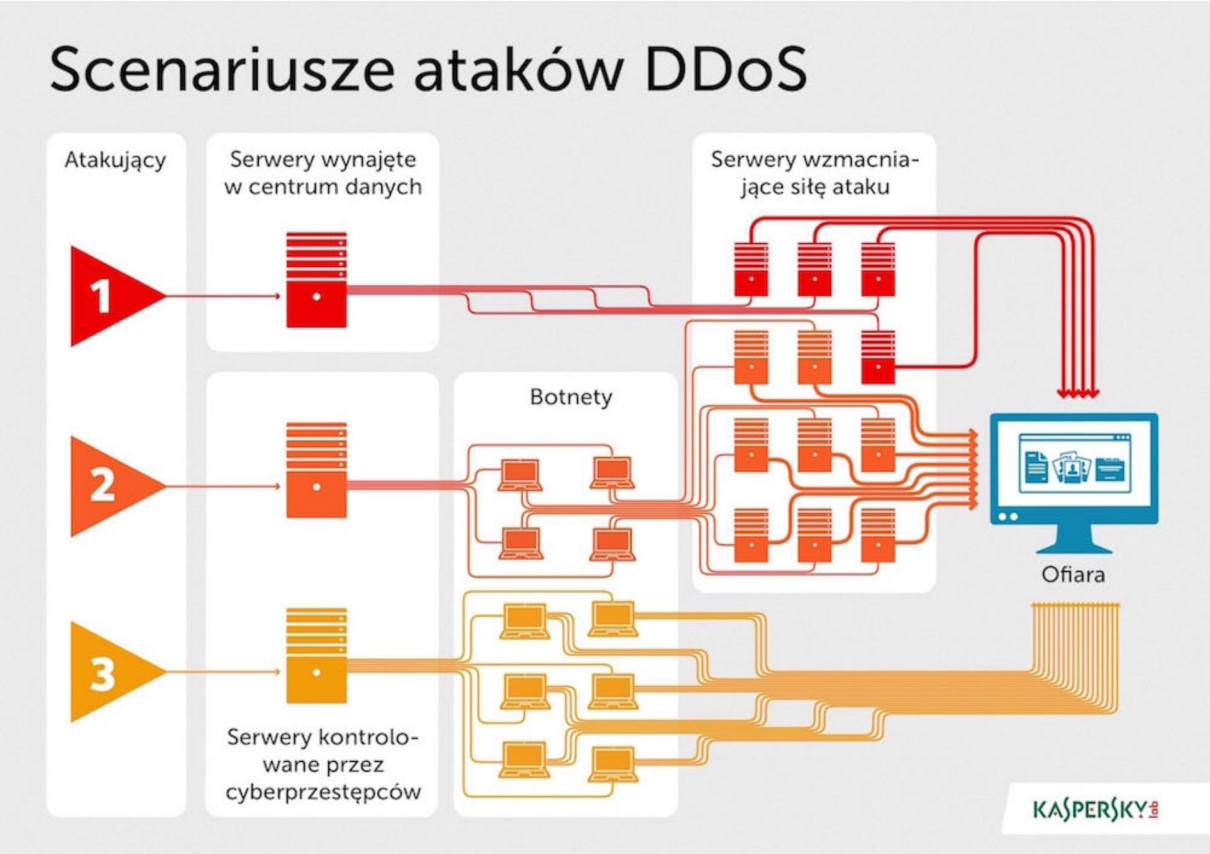
KASPERSKY DDoS PROTECTION

Ochrona firm przed atakami DDoS

Ataki Distributed Denial of Service (DDoS) to jedna z najpopularniejszych broni w arsenale cyberprzestępców. Celem takich ataków jest spowolnienie lub całkowite zatrzymanie systemów informatycznych, takich jak strony WWW lub bazy danych, co w efekcie doprowadza do braku możliwości uzyskiwania do nich dostępu przez użytkowników i klientów. Za atakiem DDoS mogą stać różne motywy, od cyberchuligaństwa przez nieczyste zagrania konkurencji aż po wymuszenia i szantaż.

Nowoczesny rynek ataków DDoS charakteryzuje się wielowarstwową strukturą. Obejmuje ludzi, którzy przeprowadzają ataki, twórców botnetów, którzy udostępniają swoje zasoby, pośredników, którzy organizują ataki i rozmawiają z ich zleceniodawcami, oraz ludzi odpowiedzialnych za stronę finansową tego cyberprzestępczego przedsięwzięcia. Celem ataku może być każdy węzeł sieciowy dostępny przez internet – konkretny serwer, urządzenie sieciowe lub nieużywany adres w podsieci ofiary.

Istnieją dwa powszechne scenariusze przeprowadzania ataków DDoS: wysyłanie żądań bezpośrednio do atakowanego zasobu z dużej liczby zainfekowanych komputerów (tzw. botów) lub wzmacnianie ataku poprzez publicznie dostępne serwery zawierające nieuaktualniane (dziurawe) systemy i aplikacje. W pierwszym scenariuszu cyberprzestępcy zamieniają wiele komputerów w tzw. maszyny zombie, które następnie postępują zgodnie z poleceniami organizatora ataku i jednocześnie wysyłają żądania do wskazanego systemu komputerowego (stąd słowo distributed – rozproszony – w nazwie ataku). Szczególnym przypadkiem takiego ataku są działania haktywistów, którzy rekrutują użytkowników i dostarczają im specjalnie przygotowane oprogramowanie, które służy do atakowania konkretnego celu.



Najpopularniejsze rodzaje ataków DDoS

W drugim scenariuszu, obejmującym wzmacnianie ataku, zamiast botów mogą zostać wykorzystane serwery wynajęte w centrach danych. Najczęściej stosowane są publiczne serwery, na których można znaleźć przestarzałe i niezałatane oprogramowanie. Wykorzystane mogą zostać zarówno serwery DNS, jak i NTP. Atak jest wzmacniany poprzez sfałszowanie zwrotnych adresów IP i wysłanie krótkiego żądania do atakowanego serwera, który potrzebuje dłuższego czasu, aby odpowiedzieć. Otrzymana odpowiedź jest wysyłana pod sfałszowany adres IP należący do ofiary.

Obecnie istnieje tak dużo szkodliwych programów i botnetów stworzonych przez cyberprzestępców, że niemal każdy może zlecić atak DDoS. Cyberprzestępcy reklamują swoje usługi, mówiąc, że każdy może wstrzymać działanie dowolnej strony WWW nawet za 50 dolarów dziennie. Opłaty są zazwyczaj dokonywane w kryptowalucie, zatem ich wyśledzenie jest niemal niemożliwe.

Przystępne ceny oznaczają, że celem ataku DDoS może stać się każdy zasób dostępny online. Problem nie dotyczy jedynie dużych i znanych organizacji czy struktur rządowych. Z punktu widzenia cyberprzestępcy zaatakowanie zasobów online dużej firmy jest znacznie trudniejsze, jednak koszt braku dostępności poniesiony przez ofiarę będzie w takim przypadku ogromny. Poza bezpośrednimi stratami wynikającymi z utraconych możliwości biznesowych (np. wstrzymanie sprzedaży w sklepie online) na ofiarę mogą zostać nałożone grzywny związane z niedopełnieniem gwarantowanej jakości usług, a dodatkowym balastem mogą być koszty przygotowania firmy na kolejne ataki. Ostatecznie reputacja ofiary może zostać poważnie naruszona, co może doprowadzić do utraty klientów.

Łączne straty wynikające z ataku DDoS różnią się w zależności od rozmiaru firmy, segmentu rynku i rodzaju zaatakowanej usługi. Zgodnie z szacunkami organizacji analitycznej IDC jedna godzina braku dostępności zasobu online to straty w wysokości 10 000 – 50 000 dolarów.

Metody walki z atakami DDoS

Na rynku istnieją dziesiątki firm świadczących usługi ochrony przed atakami DDoS. Niektóre z nich instalują u klienta rozwiązania sprzętowe, inne korzystają z możliwości oferowanych przez dostawców usług internetowych (ISP) lub przekierowują ruch internetowy klienta do specjalnych centrów czyszczenia. Mimo różnic w podejściu wszystkie te metody mają ten sam cel – odfiltrować bezużyteczny ruch generowany przez cyberprzestępców w trakcie ataku.

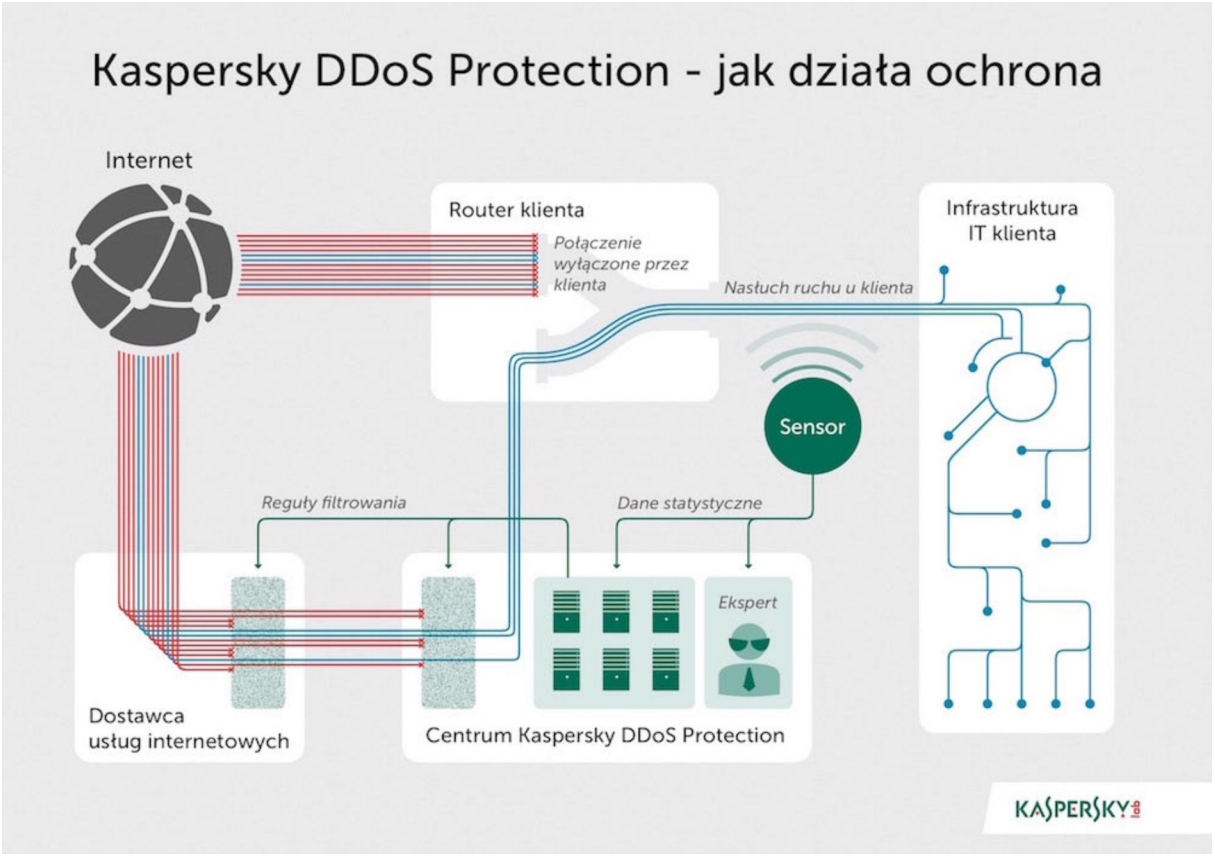
Instalowanie sprzętu sieciowego po stronie klienta jest uważane za najmniej efektywną metodę. Po pierwsze, wymaga odpowiednio przeszkolonego personelu u klienta, który będzie musiał zajmować się konserwacją urządzenia i dostosowywaniem jego ustawień, a to generuje dodatkowe koszty. Po drugie, takie podejście jest efektywne tylko w odniesieniu do ataków na usługi i nie zapobiega zagrożeniom mającym na celu zapchanie połączenia internetowego ofiary. Działająca sprawnie usługa online będzie bezużyteczna, jeżeli użytkownicy nie będą mogli dostać się do niej przez internet. Ze względu na rosnącą popularność ataków DDoS wykorzystujących wzmacnianie coraz łatwiej jest przeciążyć połączenie internetowe ofiary.

Bardziej efektywną metodą jest filtrowanie ruchu po stronie dostawcy usług internetowych, ponieważ organizacje tego typu dysponują bardzo wydajnymi łączami, których przeciążenie jest znacznie trudniejsze. Z drugiej strony jednak, dostawcy usług internetowych najczęściej nie specjalizują się w usługach bezpieczeństwa IT i usuwają z ruchu tylko to, co ewidentnie się nie przydaje. W efekcie bardziej wyrafinowany atak może wymknąć się takiemu filtrowi. Precyzyjna analiza ataku i błyskawiczna reakcja wymaga odpowiedniej wiedzy i doświadczenia. Poza tym ochrona po stronie dostawcy sprawia, że klient jest zależny od konkretnej firmy – generuje to komplikacje, gdy klient musi skorzystać z połączenia zapasowego lub przełączyć się do innego dostawcy internetu na czas ataku.

W rezultacie wyspecjalizowane centra przetwarzania ruchu wykorzystujące połączenie różnych metod filtrowania są uważane za najbardziej skuteczną metodę neutralizowania ataków DDoS.

Kaspersky DDoS Protection

Kaspersky DDoS Protection to rozwiązanie chroniące przed wszelkimi rodzajami ataków DDoS poprzez wykorzystanie rozproszonej infrastruktury centrów czyszczenia ruchu. Rozwiązanie korzysta z różnych metod, łącznie z filtrowaniem ruchu po stronie dostawcy, instalacją zdalnie kontrolowanych mechanizmów filtrujących ruch w infrastrukturze klienta oraz wykorzystaniem centrów czyszczenia danych z filtrami, które mogą być na bieżąco dostosowywane przez wyspecjalizowany personel. Dodatkowo praca rozwiązania jest nieustannie monitorowana przez ekspertów z Kaspersky Lab, dzięki czemu atak może zostać wykryty i zneutralizowany w bardzo wczesnym stadium.



Kaspersky DDoS Protection – schemat działania

Arsenał Kaspersky Lab

Kaspersky Lab już od ponad dekady skutecznie walczy z rozmaitymi zagrożeniami online. W tym czasie personel firmy nabył doświadczenie na unikatowym poziomie, łącznie ze szczegółową wiedzą dotyczącą mechanizmów funkcjonowania ataków DDoS. Eksperci z Kaspersky Lab nieustannie śledzą najnowsze trendy w internecie, analizują metody wykorzystywane do przeprowadzania cyberataków i udoskonalają mechanizmy bezpieczeństwa. Dzięki tej wiedzy i doświadczeniu możliwe jest wykrycie ataku DDoS w bardzo wczesnym stadium – zanim doprowadzi on do spowolnienia chronionego zasobu online.

Drugim elementem technologii zastosowanej w rozwiązaniu Kaspersky DDoS Protection jest sensor instalowany w infrastrukturze IT klienta. Jest to specjalistyczne oprogramowanie działające pod kontrolą systemu operacyjnego Ubuntu, a jego instalacja wymaga jedynie standardowego serwera z architekturą x86. Sensor analizuje rodzaje wykorzystywanych protokołów, liczbę wysyłanych pakietów danych, zachowanie użytkowników na stronie WWW klienta, a dokładniej metadane lub informacje dotyczące wysyłanych danych. Sensor nie przekierowuje ruchu klienta, nie modyfikuje go, ani nie analizuje zawartości jakichkolwiek wiadomości. Statystyki są następnie dostarczane do działającej w chmurze infrastruktury Kaspersky DDoS Protection, gdzie dla każdego klienta tworzony jest odpowiedni profil bazujący na zgromadzonych metadanych. W rezultacie powstaje typowy dla danego klienta wzorzec wymiany informacji. Podczas dalszej analizy ruch jest porównywany z tym wzorcem, a wykryte zmiany mogą oznaczać początek ataku DDoS.

Najważniejszy element rozwiązania Kaspersky DDoS to centra czyszczenia. Korzystają one z bezpośredniego połączenia z liniami stanowiącymi szkielet internetu w takich miejscach jak Frankfurt czy Amsterdam. Kaspersky Lab korzysta jednocześnie z kilku takich centrów, dzięki czemu ruch wymagający czyszczenia może być odpowiednio dzielony lub przekierowywany w ramach potrzeb.

Ważnym składnikiem kontroli ruchu DDoS jest filtrowanie po stronie dostawcy usług internetowych. Jego rola nie musi ograniczać się do oferowania klientowi kanału internetowego – może on zostać partnerem technologicznym Kaspersky Lab. Dzięki temu rozwiązanie Kaspersky DDoS Protection może odfiltrowywać niepotrzebny ruch – wykorzystywany w większości ataków DDoS – możliwe najbliżej źródła. W ten sposób można zapobiec połączeniu się strumieni danych w jeden potężny atak i zmniejszyć obciążenie centrów czyszczenia, które będą mogły zająć się przetwarzaniem bardziej zaawansowanych elementów ataku DDoS.

Narzędzia przekierowywania ruchu

Aby rozwiązanie bezpieczeństwa mogło funkcjonować efektywnie, konieczne jest skonfigurowanie kanału komunikacyjnego między centrami czyszczenia a infrastrukturą klienta. W rozwiązaniu Kaspersky DDoS Protection kanały te są zorganizowane zgodnie z protokołem Generic Routing Encapsulation. Służą one do przygotowania tunelu wirtualnego między centrum czyszczenia a sprzętem sieciowym klienta. Tunel ten jest wykorzystywany do dostarczania oczyszczonego ruchu do klienta.

Przekierowanie ruchu może zostać zrealizowane z użyciem jednej z dwóch metod: poprzez protokół dynamicznego trasowania BGP lub modyfikację wpisu DNS, tak by zawierał on informację o adresie URL centrum czyszczenia. Pierwsza metoda jest rozwiązaniem preferowanym, ponieważ pozwala na znacznie szybsze przekierowanie ruchu oraz zapewnia ochronę przed atakami wycelowanymi w konkretne adresy IP. Jednak wymaga ona dostępności u klienta zakresu adresów, które są niezależne od dostawcy usług internetowych.

Wybór metody ma niewielki wpływ na sam mechanizm przekierowania. Jeżeli użyta zostanie pierwsza metoda, routery BGP u klienta i w centrum czyszczenia ustanawiają permanentne połączenie poprzez tunel wirtualny. W przypadku ataku tworzona jest nowa trasa dla ruchu przepływającego z centrum czyszczenia do klienta. Jeżeli użyta zostanie druga metoda, klientowi przypisywany jest adres IP z puli centrum czyszczenia. Gdy rozpocznie się atak, klient zmienia adres IP we wpisie DNS na adres przypisany przez centrum czyszczenia. Po wykonaniu tej operacji cały ruch kierowany na adres klienta trafi najpierw do centrum czyszczenia. Jednak, aby zablokować trwający atak przeprowadzany na pierwotny adres IP, dostawca musi zablokować cały ruch z wyjątkiem tego przesyłanego przez centrum czyszczenia.

Jak to działa?

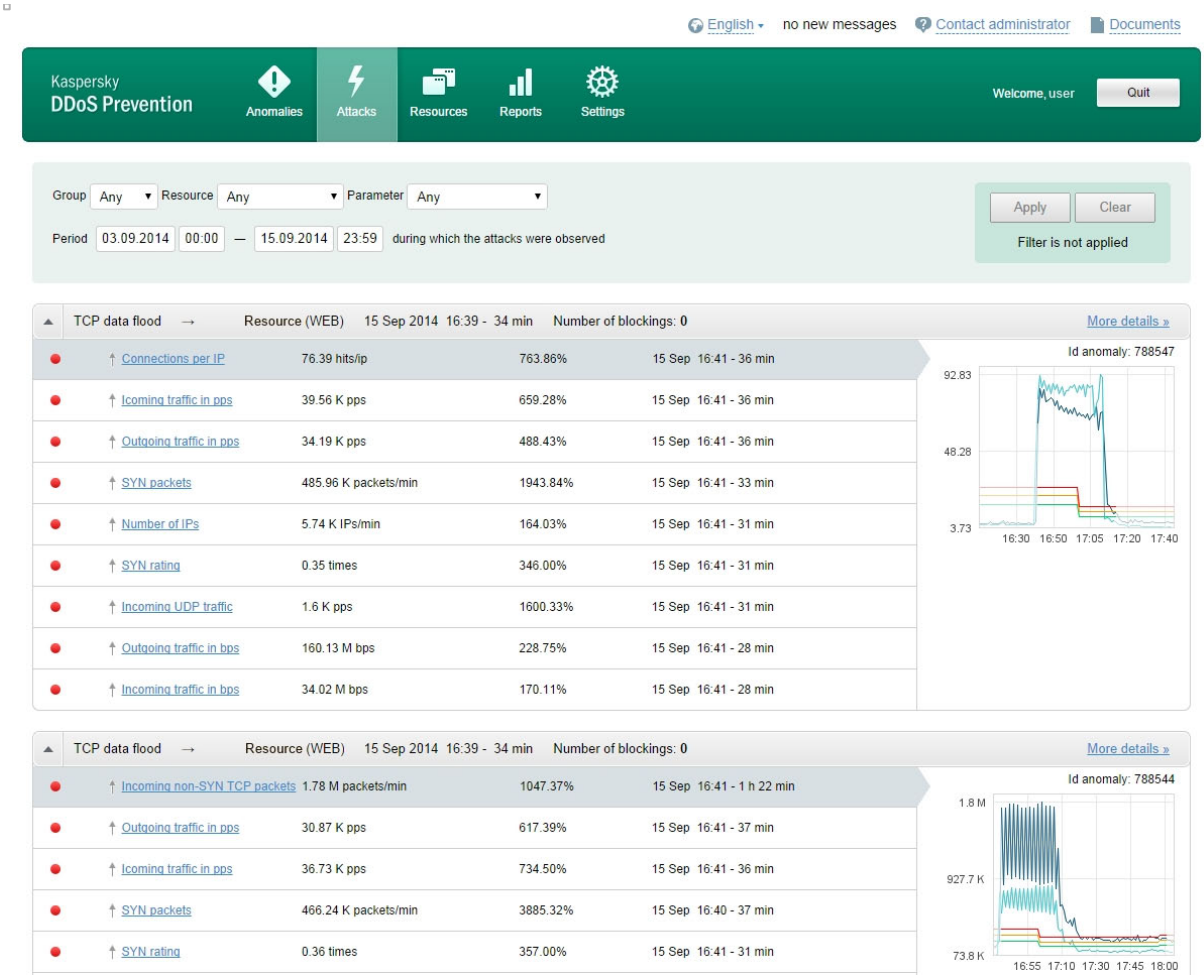
Podczas standardowej pracy cały ruch internetowy trafia bezpośrednio do klienta. Działania proaktywne rozpoczynają się, gdy sensor działający w infrastrukturze klienta wygeneruje ostrzeżenie. W pewnych przypadkach analitycy z Kaspersky Lab wiedzą o ataku już w momencie jego rozpoczęcia się i natychmiast informują o tym klienta. W takiej sytuacji kroki zapobiegawcze mogą zostać podjęte z wyprzedzeniem. Dyżurny ekspert Kaspersky Lab ds. ochrony przed atakami DDoS otrzymuje sygnał, że ruch docierający do klienta nie jest zgodny z utworzonym wcześniej profilem statystycznym. Jeżeli atak zostanie potwierdzony, informacja jest przekazywana do klienta, a ten powinien wydać dyspozycję przekierowania ruchu do centrów czyszczenia (umowa z klientem może obejmować zapis gwarantujący wykonanie takiego przekierowania w sposób automatyczny).

Gdy technologie Kaspersky Lab zidentyfikują rodzaj ataku, natychmiast stosowane są odpowiednie reguły czyszczenia (w zależności od atakowanego zasobu online). Niektóre reguły, przeznaczone do walki z najbardziej zaawansowanymi atakami, są przesyłane do infrastruktury dostawcy usług internetowych i stosowane na routerach stanowiących własność dostawcy. Pozostały ruch jest dostarczany do centrów czyszczenia i jest filtrowany zgodnie z szeregiem parametrów, takich jak adresy IP, dane geograficzne, informacje z nagłówków http czy poprawność protokołów i wymiany pakietów SYN.

Sensor kontynuuje monitorowanie ruchu, który dociera do klienta. Jeżeli w dalszym ciągu zawiera on jakiekolwiek oznaki ataku DDoS, sensor ostrzega centrum czyszczenia i ruch poddawany jest głębokiej analizie behawioralnej oraz wykorzystującej sygnatury. W oparciu o te metody możliwe jest odfiltrowanie szkodliwego ruchu – np. na podstawie zaobserwowanych parametrów rozwiązanie może całkowicie zablokować określony rodzaj ruchu lub konkretne adresy IP. Dzięki takiemu podejściu możliwe jest zablokowanie nawet najbardziej wyrafinowanych działań cyberprzestępców, łącznie z atakiem HTTP flood polegającym na imitowaniu użytkownika, który odwiedza atakowaną stronę w sposób

chaotyczny i nienaturalnie szybki. Ataki takie są najczęściej przeprowadzane z użyciem ogromnej ilości maszyn zombie.

Eksperci z Kaspersky Lab monitorują cały proces przy użyciu specjalnego interfejsu. Jeżeli atak jest bardziej skomplikowany niż typowe działania cyberprzestępców lub parametry wskazują na nietypową aktywność, ekspert może wkroczyć do akcji, zmienić reguły filtrowania i zreorganizować mechanizm ochrony, by odeprzeć nową formę zagrożenia. Ponadto klient jest wyposażony we własny interfejs, przy użyciu którego może obserwować funkcjonowanie rozwiązania oraz parametry ruchu.



Zrzut ekranu z interfejsu Kaspersky DDoS Protection (interfejs dla klienta)

Gdy atak dobiegnie końca, ruch jest kierowany z powrotem do serwerów klienta. Kaspersky DDoS Protection powraca do stanu czuwania, a klient otrzymuje szczegółowy raport dotyczący ataku, wykresy demonstrujące zmierzone parametry oraz rozkład geograficzny źródeł ataku.

Korzyści płynące z podejścia stosowanego przez Kaspersky Lab

Metoda polegająca na przekierowaniu ruchu podczas ataku do centrów czyszczenia Kaspersky Lab i filtrowaniu ruchu po stronie ISP pozwala na znaczną redukcję kosztów przeznaczonych na ochronę przed atakami DDoS.

Reguły filtrowania są tworzone indywidualnie dla klienta w oparciu o specyfikę jego usług online, które mają zostać objęte ochroną.

Eksperci z Kaspersky Lab nieustannie monitorują proces ochrony, dzięki czemu mogą dostosować parametry filtrowania, gdy zajdzie taka potrzeba.

Bliska współpraca między ekspertami ds. rozwiązania Kaspersky DDoS Protection i programistami z Kaspersky Lab umożliwia dostosowywanie ochrony w odpowiedzi na zmieniający się krajobraz ataków.

W celu zapewnienia możliwie najwyższego poziomu niezawodności Kaspersky Lab wykorzystuje jedynie europejski sprzęt i dostawców usług w zakresie filtrowania i monitorowania ruchu w krajach europejskich. Wszystkie centra filtrowania ruchu znajdują się w Europie, a analizowane przez serwis metadane dotyczące ruchu klienta nigdy nie wychodzą poza terytorium Unii Europejskiej.

Kaspersky Lab posiada bogate doświadczenie w ochronie przed atakami DDoS. Z rozwiązań firmy korzysta już wiele instytucji finansowych, organizacje rządowe i komercyjne, sklepy online itd.