Grzegorz Górski
Mateusz Wojsa
Zakład Systemów Multimedialnych i Sztucznej Inteligencji
Wydział Elektroniki i Informatyki
Politechnika Koszalińska
ul. J.J. Śniadeckich 2
75-453 Koszalin

Blokowanie usług operatora sieciowego – przegląd wybranych ataków i metod ochrony

Słowa kluczowe: usługi internetowe, ataki sieciowe, blokowanie usług

1. Wprowadzenie

Większość powszechnie stosowanych protokołów sieciowych warstwy aplikacji powstała w czasach, kiedy kwestie związane z bezpieczeństwem transmisji danych nie miały dużego znaczenia. Nikt tak naprawdę nie spodziewał się tak szybkiego wykorzystania tych narzędzi przez cyberprzestępców. Dziś oczywiście nie ma możliwości zmiany fundamentów owych protokołów, przynajmniej jeżeli patrzymy na to krótkoterminowo.
Jednakże prócz problemów związanych z kompromitacją danych poufnych, protokoły te są praktycznie bezsilne na ataki, na jeden z fundamentów bezpieczeństwa informacji, czyli dostępność.

2. Rodzaje ataków

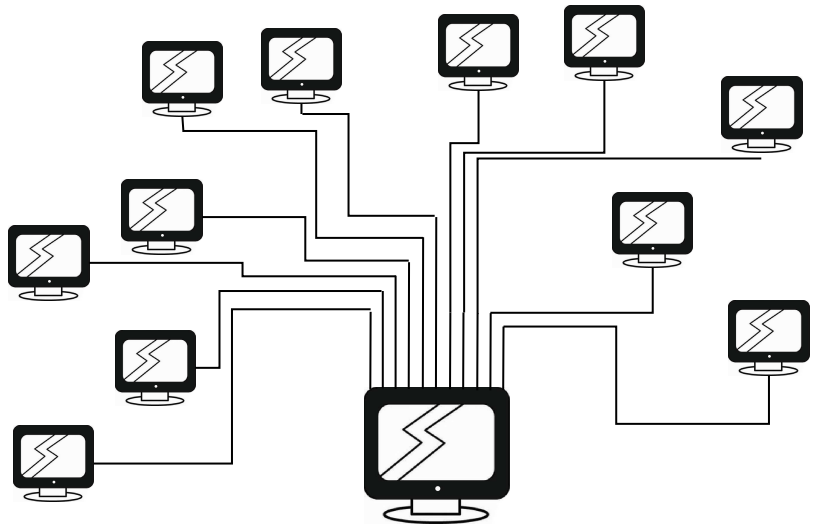
Atak a raczej cyberatak, jest to ciąg działań podjętych w celu zakłócenia, przejęcia danych bądź uzyskania kontroli nad danym systemem. Rodzajów ataków oraz ich wariacji jest wiele. Autorzy przedstawiają kilka podstawowych ataków oraz metody, które znacznie przeciwdziałają ich skutecznemu przeprowadzeniu.

2.1. Ataki których celem jest zablokowanie usług operatora

2.1.1. Botnet

Botnet jest to sieć zainfekowanych komputerów, która udostępnia hakerowi zdalną kontrolę nad zainfekowanymi maszynami. Dzięki kontroli nad setkami czy

nawet tysiącami maszyn, haker może rozsyłać różnego rodzaju kontent począwszy od spamu, a kończąc na wirusach, kraść dane osobowe, czy nawet przeprowadzać ataki DDoS. Botnety to jedno z największych współczesnych zagrożeń IT. Ich rosnąca popularność wśród cyberprzestępców wynika z ich zdolności do infiltracji niemal każdego urządzenia podłączonego do Internetu. Wykorzystuje się je nawet do „kopania" kryptowalut, które w ostatnich latach zyskały na popularności a cena niektórych wzrosła tysiące razy.



Aby lepiej zrozumieć działanie botnetów, należy wziąć pod uwagę, że sama nazwa to połączenie dwóch członów "robot" oraz "sieć". W szerokim tego słowa znaczeniu botnet jest to sieć robotów wykorzystywanych do popełniania cyberprzestępczości. Cyberprzestępcy je kontrolujący nazywani są pasterzami lub botmasterami.

Aby zbudować botnet, botmasterzy potrzebują jak najwięcej zainfekowanych urządzeń pod ich komendą. Im więcej botów jest podłączonych, tym większy botnet. Im większy botnet, tym większy wpływ i możliwa większa skala ataku. Rozmiar w tym przypadku ma znaczenie i to kolosalne. Ostatecznym celem przestępcy najczęściej jest zysk finansowy, propagowanie szkodliwego oprogramowania lub po prostu wprowadzenie ogólnego chaosu w Internecie.

Botnety zazwyczaj są tworzone nie tylko w celu złamania pojedynczego komputera. Charakteryzują się tym, iż zostały zaprojektowane do infekowania wielu urządzeń, liczonych nawet w milionach. Do zainfekowania komputera dochodzi najczęściej za pośrednictwem koni trojańskich. Strategia dostarczenia konia trojańskiego na komputer ofiary wymaga od użytkownika zainfekowania własnego systemu np. poprzez otwieranie załączników wiadomości e-mail ze złośliwym

oprogramowaniem, klikanie złośliwych wyskakujących reklam lub pobieranie niebezpiecznego oprogramowania. Gdy urządzenia są już zainfekowane, botnety mogą uzyskiwać dostęp i modyfikować dane, atakować inne komputery, czy też popełniać inne przestępstwa. Bardziej złożone botnety mogą nawet automatycznie się rozprzestrzeniać, wyszukiwać oraz infekować urządzenia.

Botnety są trudne do wykrycia. Ograniczają swoją pracę używając tylko niewielkiej ilości mocy obliczeniowej, by uniknąć zakłóceń normalnych funkcji urządzenia, co mogłoby do prowadzić do ostrzeżenia użytkownika. Bardziej zaawansowane botnety są zaprojektowane tak, aby aktualizować swoje zachowanie. Zachowanie to znacznie utrudnia wykrywanie ich przez oprogramowanie cyberbezpieczeństwa. Użytkownicy nie zdają sobie sprawy, że ich urządzenie jest w tym samym czasie kontrolowane przez botmastera. Usunięcie komputera z botnetu, wiąże się z usunięciem złośliwego oprogramowania, które kontroluje maszynę.

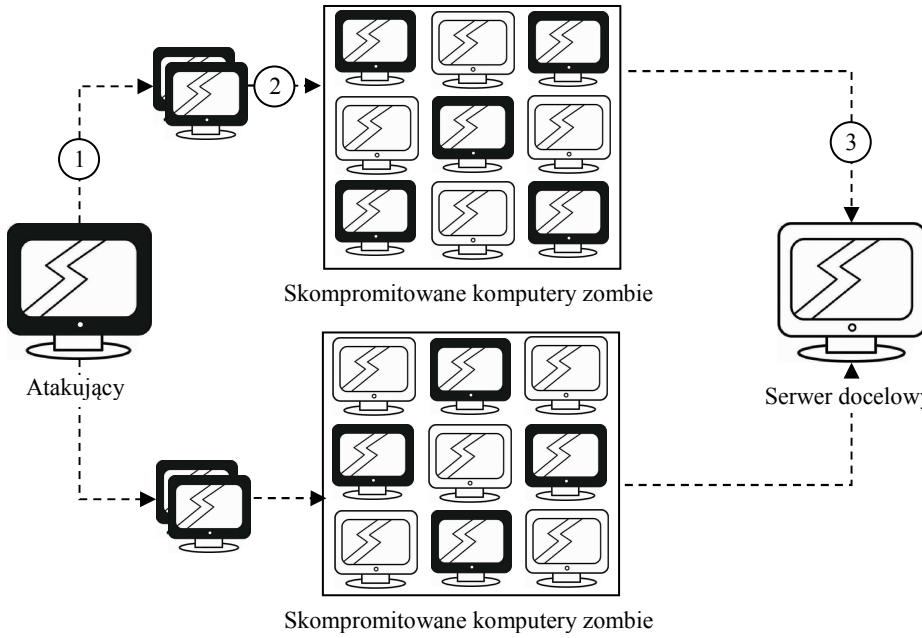
Przeprowadzenie ataku odmowy dostępu do usługi jest dość proste z wykorzystaniem Botnetu. Duża masa pozwala na generowanie dużej ilości żądań w sieci, a co za tym idzie zalanie nimi ofiary, przez co usługa usługodawcy zostaje zdestabilizowana.

2.1.2. DDoS

Jest atakiem na komputer lub sieć, którego celem jest zmniejszenie, ograniczenie bądź zablokowanie dostępu do zasobów systemowych użytkownikom. Atak ten bazuje na ataku DoS, którego celem jest destabilizacja pracy systemu, przeładowując jego zasoby za pomocą nieuzasadnionych żądań.

Istnieje wiele kategorii ataków:

- Volumetric Attack
- Fragmentation Attack
- TCP State-Exhaustion Attack
- Application Laer Attack



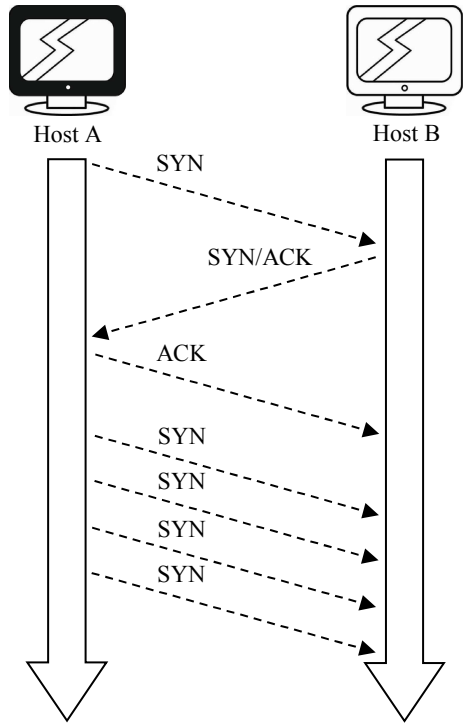
Przebieg ataku:

1. Atakujący instruuje kontrolery.
2. Kontrolery infekują dużą ilość komputerów.
3. Poinstruowane komputery zombie zalewają żądaniami serwer docelowy.

Koszt przeprowadzenia ataku DDoS jest stosunkowo niewielki, a co za tym idzie jest łatwy do zorganizowania. Stosowany jest najczęściej jako dywersja. Napływające żądania skutecznie potrafią odwrócić uwagę personelu IT, a tym samym znacznie podnoszą prawdopodobieństwo skutecznego przeprowadzenia właściwego ataku by mógł odnieść oczekiwany skutek.

2.1.3. SYN Flooding

Podczas gdy nowoczesne systemy operacyjne są lepiej przygotowane do zarządzania zasobami, co utrudnia przepełnienie tabel połączeń, serwery nadal są narażone na ataki typu SYN Flooding.



SYN Flooding bazuje na wadzie implementacji three-way handshake przez większość hostów. Kiedy host B odbiera żądanie SYN od hostu A, musi utrzymywać częściowo otwarte połączenie w liście „kolejki odsłuchowej" przez określony czas. Zasadniczo, sprawca wysyła żądania połączenia TCP szybciej niż maszyna docelowa może je przetworzyć. Kolejka odsłuchowa ofiary szybko się zapełnia, co powoduje nasycenie sieci. Zdolność zatrzymywania każdego niecałkowitego połączenia, może być wykorzystana do wykonania ataku DoS.

2.1.3.1. Przebieg ataku

Kiedy klient i serwer ustanawiają normalny "trójdrożny uścisk dłoni" TCP, wymiana wygląda następująco:

1. Klient żąda połączenia, wysyłając komunikat SYN (synchronizacja) do serwera. Najczęściej atakujący w celu anonimizacji swojego ruchu wykorzystuje fałszywy adres IP.
2. Serwer potwierdza, wysyłając wiadomość SYN-ACK (potwierdzenie synchronizacji) do klienta.
3. Klient odpowiada komunikatem ACK (potwierdzenie), a połączenie zostaje ustanowione.

W ataku powodzi SYN, atakujący wysyła powtarzające się pakiety SYN do każdego portu na docelowym serwerze. W tym czasie serwer nie może zamknąć połączenia, wysyłając pakiet RST, a połączenie pozostaje otwarte.

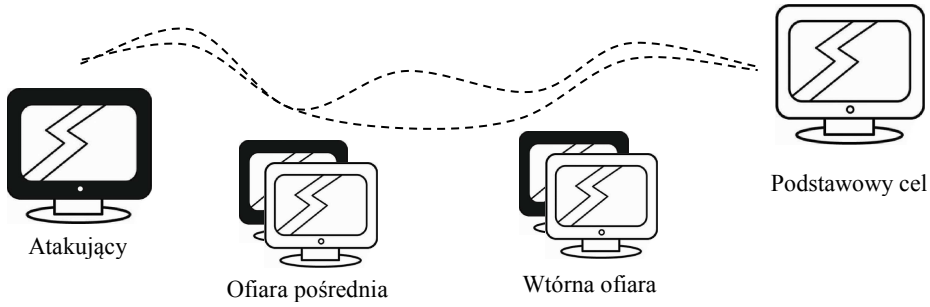
Zanim upłynie limit czasu połączenia Serwer, nieświadomy ataku, otrzymuje wiele pozornie uzasadnionych próśb o nawiązanie komunikacji. Odpowiada na każdą próbę pakietem SYN-ACK z każdego otwartego portu. Pozostawia to coraz więcej połączeń na wpół otwartych. Złośliwy klient albo nie wysyła oczekiwanego ACK, a atakowany serwer będzie czekał na potwierdzenie swojego pakietu SYN-ACK. W końcu, gdy wypełnią się tablice przepełnienia połączenia serwera, usługa dla legalnych klientów zostanie odrzucona, a serwer może nawet działać nieprawidłowo lub ulec awarii.

Pakiety SYN są często używane, ponieważ najmniej prawdopodobne jest, że zostaną odrzucone domyślnie.

2.1.4. DRDoS połączenie dwóch powyższych

DRDoS jest to odmiana ataku odmowy dostępu DoS. Powstała w wyniku połączenia metody zalewania żądaniami synchronizacji oraz metod używanych przy rozproszonych atakach odmowy dostępu DDoS.

Atak ten polega na generowaniu specjalnych pakietów SYN. Ich adres źródłowy jest oczywiście fałszywy ponieważ jest nim adres ofiary. Następnym krokiem jest wysłanie dużej ilości takich pakietów do sieci. Komputery, do których zostały zaadresowane, odpowiadają pakietami SYN/ACK. Pakiety SYN/ACK, są kierowane na adres pochodzący z fałszywego nagłówka. W wyniku czego ofiara jest zalewana olbrzymią liczbą pakietów, pochodzących z wielu hostów. W porównaniu do tradycyjnego ataku typu DDoS, utrudnia to wykrycie rzeczywistego źródła ataku.



Przebieg ataku:

1. Atakujący rozpoczyna atak wysyłając żądanie do ofiar pośrednich
2. Żądanie zostaje przekierowane do ofiar wtórnych
3. Cel zostaje zaatakowany przez ofiary wtórne

Protokół TCP został zaprojektowany w taki sposób, że przed transmisją danych zapewnia:

- że przed transmisją danych cel jest gotowy do odbioru informacji ("uzgadnianie")
- że po transmisji wszystkie dane zostały odebrane ("ACK").

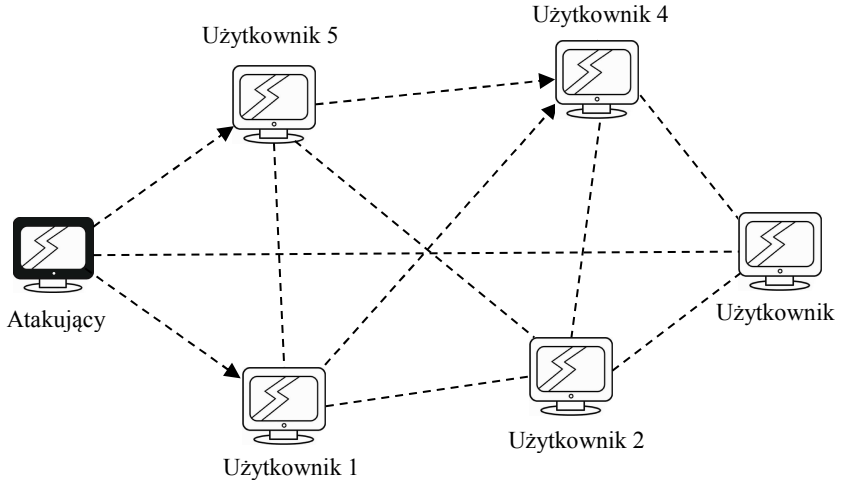
"Uścisk dłoni" można wypróbować kilka razy z rzędu. Dla żądania otwarcia sesji TCP ("SYN"), sfałszowany odbiorca pakietów otrzyma kilka prób otwarcia sesji. Im wyższy jest współczynnik wzmocnienia między rozmiarem minimalnego żądania a rozmiarem odpowiedzi, tym bardziej efektywny jest DRDoS.

Możliwe jest również wykonanie tego rodzaju wzmocnienia za pomocą protokołu UDP. Jego rolą jest umożliwienie transmisji danych między dwiema jednostkami. Jest jednym z głównych protokołów używanych w sieci Internet. Dzięki UDP atakujący może ukryć źródło ataku, poprzez użycie adresu IP osoby trzeciej w celu odbicia pakietów (fragmentacja przesyłanych danych).

Atakujący wysyła żądania odpowiedzi na różne serwery. Żądanie posiada zmodyfikowany adres IP celu, tzn. nie jest to adres własny atakującego, a adres atakowanego. Cel otrzymuje ogromne fale pakietów ze wszystkich serwerów, co skutkuje zdestabilizowaniem środowiska.

2.1.5. Peer to Peer atack

Sieci peer-to-peer różnią się do tradycyjnych sieci klient-serwer pod wieloma aspektami. Jednym z najważniejszych jest to, że każdy peer działa jako serwer i klient sieci. Innymi słowy w owych sieciach nie ma centralnego serwera służącego do przechowywania i udostępniania plików. Sieci peer-to-peer zawierają zdecentralizowane struktury ad hoc. Topologia sieci zmienia się co chwilę na wskutek możliwości losowego opuszczenia oraz dołączania do sieci przez uczestnika. Cechy te sprawiają, że jest ona podatna na ataki m.in. takie jak DoS.



Sieci P2P składają się z dużej liczby jednocześnie działających hostów. Tak więc jeden lub więcej złośliwych węzłów sieci, może z łatwością wykonywać DoS lub DDoS, czyli próbę zalania sieci fałszywymi pakietami, uniemożliwiając w ten sposób legalny ruch sieciowy. Inną metodą jest zalanie ofiary żądaniami kalkulacji w taki sposób, aby był na tyle zajęty by nie mógł odpowiedzieć na inne żądania. Ataki DoS są znacznie bardziej efektywne, jeśli w atak zaangażowanych jest wiele hostów (rozproszona odmowa usługi). W DDoS atakującymi komputerami są często komputery osobiste z dostępem do połączenia Internet, które zostały zainfekowane przez wirusa lub trojana. Sprawca może zdalnie nimi sterować oraz kierować atakiem na dowolny host. Atak DDoS można jeszcze bardziej wzmocnić stosując nieskompromitowane hosty jako wzmacniacze. Zombie wysyłają żądania do nieskompromitowanych hostów i podszywają swój adres IP adresem IP ofiary. Kiedy nieskompromitowani gospodarze odpowiadają, wyślą pakiety odpowiedzi do ofiary. Jest to tak zwany atak refleksyjny.

Sieci P2P do udostępniania plików nie są nowe. Ich wykorzystanie do dzielenia się wszystkimi mediami przez Internet, umożliwia „wybuch” w zapisach na stacjach roboczych. To była tylko kwestia czasu, kiedy cyberprzestępcy zaczęli wykorzystywać te "publiczne" sieci.

Wykrywanie ataku DoS P2P jest łatwe, lecz obrona przed nim jest trudna. Obrony obwodowe organizacji byłyby przytłoczone tak dużym atakiem. Blokowanie dużej liczby źródłowych adresów IP jest czasochłonne i spowolniłoby przetwarzanie pakietów do indeksowania. Jednym z rozwiązań jest zapobieganie w pierwszej kolejności docieraniu pakietów do sieci biznesowej.

2.1.6. Metody zapobiegawcze

Głównymi metodami zapobiegawczymi, są systemy detekcji bazujące na identyfikacji oraz dyskryminacji nielegalnego wzrostu ruchu z legalnego ruchu pakietowego. Systemy te kategoryzują atak jako zjawisko anormalne poprzez zbieranie statystyk ruchu sieciowego oraz badanie jego trendu.

Dobrą praktyką jednakże wymagającą wcześniejszego planowania jest budowa infrastruktury, w taki sposób by można było zarezerwować dodatkową nadmiarową pojemność, która byłaby w stanie wchłonąć atak poprzez przekierowanie części ruchu.

Należy również zidentyfikować krytyczne usługi i zatrzymać te, które nie są wykorzystywane. Należy mieć zawsze zainstalowane oraz zawsze aktualne aplikacje antywirusowe oraz antymalware'owe. Świadomość zespołu IT jest również jednym z ważniejszych elementów, dlatego należy dbać o szkolenia związane z bezpieczeństwem. Jeżeli atak został przeprowadzony skutecznie to ostatecznym krokiem jest zamknięcie wszystkich usług, w których wystąpił atak.

3. Podsumowanie

Niezależnie od rodzaju i wielkości przemysłu, firmy na całym świecie coraz częściej stają się celem ataków DDoS. Wyrafinowanie i intensywność tych ataków rośnie wykładniczo ze względu na wzrost w liczbie zaatakowanych systemów oraz niezałatanych luk w zabezpieczeniach.

Rozpoczęcie ataku DDoS jest trywialne w porównaniu do ilości czasu i zasobów poświęconych na stworzenie skutecznego środka zaradczego. Nowe techniki wykrywania i zwalczania tych ataków, są nieustannie tworzone, jednak tworzone są również nowe formy ataków, które powodują, że środki zaradcze stają się przestarzałe. Jest to problem, który aktualnie nie ma trwałego rozwiązania.

Bibliografia

1. Lei Xue, Xiaobo Ma , Xiapu Luo, Edmond W. W. Chan , Tony T. N. Miu, Guofei Gu, „Toward Detecting Target Link Flooding Attacks”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Volume 13, Issue 10, Pages 2423-2438, OCT 2018
2. Murat Semerci, Ali Taylan Cemgil, Bulent Sankur, „An intelligent cyber security system against DDoS attacks in SIP networks”, COMPUTER NETWORKS, Volume 136, Pages 137-154, MAY 8 2018

3. Ivica Dodig, Vlado Sruk, Davor Cafuta, „Reducing false rate packet recognition using Dual Counting Bloom Filter", TELECOMMUNICATION SYSTEMS, Volume 68, Issue 1, Pages 67-78, MAY 2018
4. Mutaz H. H. Khairi, Sharifah H. S. Ariffin, N. M. Abdul Latiff, A. S. Abdullah, M. K. Hassan, „A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN)", ENGINEERING TECHNOLOGY & APPLIED SCIENCE RESEARCH, Volume 8, Issue 2, Pages 2724-2730, APR 2018
5. Ademola P. Abidoye, Ibidun C. Obagbuwa, "DDoS attacks in WSNs: detection and countermeasures", ET WIRELESS SENSOR SYSTEMS, Volume 8, Issue 2, Pages 52-59, APR 2018
6. Yong-Joon Lee, Nam-Kyun Baik, Cheonshik Kim, Ching-Nung Yang, „Study of detection method for spoofed IP against DDoS attacks", PERSONAL AND UBIQUITOUS COMPUTING, Volume 22, Issue 1, Pages 35-44, Special Issue SI, FEB 2018
7. Silva, S., Silva, R., Pinto, R., Salles, R. M., „Botnets: A survey", Computer Networks, Volume 57, Issue 2, Pages 378-403, 4 February 2013
8. Materiały szkoleniowe EC-Council do egzaminu CEH v9 (Certified Ethical Hacker)

Streszczenie

Udany atak na usługę internetową zwykle kojarzy się z kompromitacją danych poufnych, jednakże nie musi tak być zawsze. Celem ataków z rodziny DoS nie jest uszkodzenie czy przechwycenie danych, a utrudnienie, bądź nawet uniemożliwienie dostępu do nich. Okazało się, że u usługodawców, mogą spowodować równie kosztowne straty.

Autorzy przedstawili przegląd wybranych ataków, których celem jest zablokowanie usług udostępnianych przez operatora oraz wybrane metody minimalizujące ich skutki.

Abstract

A successful attack on an internet service is usually associated with the embarrassment of confidential data, but it does not always have to be that way. The purpose of DoS attacks is not to damage or intercept data, but to hinder or even prevent access to them. It turned out that the service providers can also cause costly losses. The authors presented an overview of selected attacks that aim to block the services provided by the operator and selected methods minimizing their effects.

Keywords: internet services, network attacks, services blocking