Mgr inż. Paweł Szynkiewicz
Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy
e-mail: pawel.szynkiewicz@nask.pl

DETEKCJA I MITYGACJA ATAKÓW DDoS GENEROWANYCH PRZEZ SIECI BOTNET

Streszczenie

Ataki typu DDoS stanowią obecnie istotne zagrożenie dla infrastruktury sieciowej oraz systemów informatycznych. Z każdym rokiem obserwowany jest wzrost pod względem liczby i skali ataków. Zwiększający się potencjał ataków DDoS jest konsekwencją istnienia rozległych sieci botnet, zdalnie kontrolowanych przez cyberprzestępców, które stanowią narzędzie do przeprowadzania tego typu ataków. W związku z tym konieczne jest ciągłe doskonalenie mechanizmów obronnych oraz opracowywanie skutecznych strategii przeciwdziałania. W artykule prezentowane jest autorskie rozwiązanie do detekcji i mitygacji ataków DDoS. Proponowana metoda działa w oparciu o sygnatury ataku, podejście rzadko stosowane w przypadku ataków DDoS. Procedura generowania sygnatur zakłada wykorzystanie danych pozyskiwanych z Teleskopu Sieciowego (darknet). Stosowana jest do tego metoda identyfikacji (fingerprinting) botnetów na podstawie pakietów sieciowych. Idea i proces tworzenia sygnatur został opisany, i poparty przykładem. Artykuł zawiera ogólny opis wykorzystywanych technologii i sposobu implementacji prezentowanej metody.

Słowa kluczowe: cyberbezpieczeństwo, DDoS, sygnatury, Botnet

WPROWADZENIE

Atak DDoS (ang. *Distributed Denial of Service*) to rodzaj cyberataku, którego celem jest zakłócenie lub całkowite zablokowania dostępu do usługi sieciowej dla prawdziwych użytkowników. Sprawcy wykorzystują dużą liczbę urządzeń podłączonych do Internetu, aby zalać serwery lub sieć ofiary (ataki wolumetryczne) fałszywymi żądaniami. Prowadzi to zwykle do przeciążania docelowego systemu przez zajęcie wszystkich wolnych zasobów infrastruktury. Ataki DDoS stają się coraz powszechniejszym i bardziej istotnym zjawiskiem w obszarze cyberbezpieczeństwa[1]. Szczególnie niebezpieczne są ataki przeprowadzane za pomocą sieci botnet (Mirai, Mantism, Zeus), czyli kontrolowanej przez cyber-przestępców i zwykle bardzo licznej grupy

[1] S. Dong, K. Abbas, R.,Jain, A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments, https://doi.org/10.1109/ACCESS.2019.2922196 (dostęp: 17.01.2025).

zainfekowanych urządzeń, wykorzystywanych do masowego generowania złośliwego ruchu sieciowego. Ofiarami takich ataków padają zarówno największe serwisy internetowe, jaki i strony rządowe. Przykłady obejmują ataki na serwisy Twitter, GitHub i Netflix, oraz strony rządowe Stanów Zjednoczonych czy brytyjskiego National Health Service (NHS)[2].

W obliczu ciągłego ryzyka wystąpienia ataków typu DDoS, konieczne jest nieustanne doskonalenie systemów bezpieczeństwa oraz poszukiwanie innowacyjnych metod obrony, które pozwolą przewidzieć i skutecznie zneutralizować potencjalne zagrożenia. Zaprezentowane w artykule rozwiązanie stanowi innowacyjne podejście do wykrywania ataków typu DDoS powodowanych przez botnety. Podejście wykorzystuje dane pochodzące z unikatowego źródła, jakim jest Teleskop Sieciowy, do generowania sygnatur pakietów wychodzących z sieci botnet. Opisana jest realizacja prezentowanego rozwiązania, w której wykorzystano nowoczesną technologię jądra Linux do zapewnienia wysokiej wydajności i elastyczności.

SYGNATURY ATAKÓW DDoS

Sygnatura ataku to unikalny wzorzec lub charakterystyka identyfikująca określony rodzaj ataku lub szkodliwej aktywności w sieci. Jest to rodzaj opisu, który zawiera cechy charakterystyczne danego rodzaju ataku, takie jak określone wzorce zachowań, sekwencje danych, adresy źródłowe IP, itp. Sygnatury ataków są wykorzystywane przez systemy bezpieczeństwa sieciowego do wykrywania i blokowania szkodliwego ruchu sieciowego, umożliwiając szybką reakcję na potencjalne zagrożenia. Efektywność tych systemów zależy w głównej mierze od doboru odpowiedniego typu sygnatur do od klasy ataków.

Najbardziej popularne systemy sygnaturowe IDS/IPS (ang. *Intrusion Detection/Prevention System*) takie jak Snort[3] czy Suricata[4] nie są w stanie zapewnić skutecznej ochrony przed wolumetrycznymi atakami DDoS. Wynika to z ograniczeń związanych z przetwarzaniem dużej ilości danych w krótkim czasie. Systemy te analizują zawartość (ang. *payload*) każdego pakietu sieciowego pod kątem wzorców ataku. Nie jest to optymalne podejście w przypadku ataków DDoS, których to pakiety nie muszą się różnić od tych typowych dla normalnego ruchu.

Efektywna detekcja ataków DDoS wymaga więc przyjęcia innej strategii przy konstrukcji i wyborze cech sygnatury ataku. Mała popularność takich rozwiązań wskazuje, że nie jest to zadanie proste. Znalezienie wzorca jednoznacznie i dostatecznie precyzyjnie identyfikującego konkretny atak DDoS może okazać się niemożliwe. Główne przyczyny to: (i) złożoność ataków i częste zmiany taktyki ataku, (ii) dynamiczne środowisko jakim są sieci komputerowe zniekształcają obraz ataku, (iii) duża ilość danych związanych z atakiem komplikuje analizę.

[2] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: Mirai and Other Botnets, „Computer" 2017, vol. 50, no. 7, s. 80-84, doi: 10.1109/MC.2017.201.
[3] https://www.snort.org/
[4] https://suricata.io/

Prezentowane podejście wykorzystuje sygnatury unikatowych wzorców ruchu sieciowego, które są charakterystyczne dla pakietów generowanych przez sieci botnet. Do generowania sygnatur wykorzystywana jest infrastruktura Teleskopu Sieciowego NASK[5] (Naukowa i Akademicka Sieć Komputerowa). Teleskop sieciowy zapewnia dostęp do cennych i trudno dostępnych danych o trwających kampaniach cyberataków realizowanych na masową skalę w sieci Internet. Analizując te dane, jesteśmy w stanie wyodrębnić i wygenerować specyficzne sygnatury ataków DDoS na poziomie pojedynczych pakietów sieciowych. Wzorce ruchu widoczne są w samych nagłówkach, nie ma więc potrzeby przetwarzania całych pakietów. Ewentualne problemy z dostępem do Teleskopu Sieciowego, który nie jest łatwo dostępnym źródłem danych, można rozwiązać zastępując go odpowiednio dużą liczbę Honeypotów[6].

TELESKOP SIECIOWY

Teleskop sieciowy (znany również jako *darknet*) to niewykorzystana przestrzeń adresów IP, które są używane wyłącznie w celu pasywnego monitorowania[7]. Nieprzydzielone adresy IP nie powinny otrzymywać żadnego ruchu sieciowego. W praktyce dzieje się jednak inaczej. Cały ruch obserwowany przez teleskop sieciowy, jest więc anomalią i z definicji klasyfikowany jest jako podejrzany.

Może być on wynikiem szerokiego zakresu zdarzeń lub działań, takich jak:

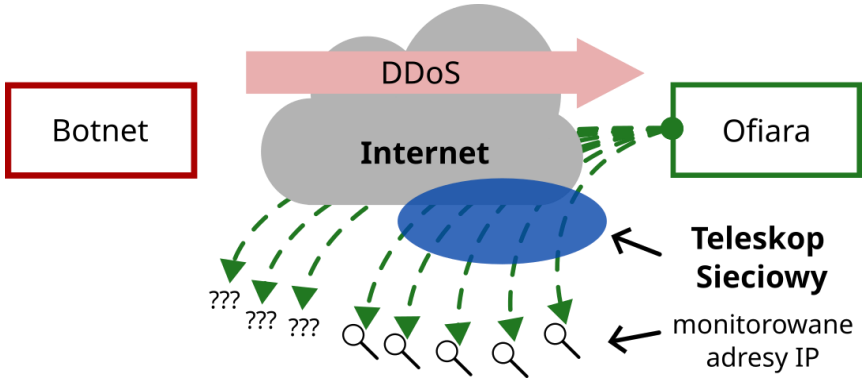
- skanowanie przestrzeni adresowej przez atakujących,
- szukanie celów podatnych na ataki przez złośliwe oprogramowanie,
- automatyczne rozprzestrzenianie się robaków internetowych,
- błędy w konfiguracji (np. błędne wpisanie adresu IP lub przestarzałe rekordy DNS),
- echa ataków DDoS.

Teleskopy sieciowe są cennym źródłem informacji o bieżących wydarzeniach w całej infrastrukturze internetowej, jednak dostęp do tych danych jest ograniczony. Infrastrukturą zarządzają zazwyczaj instytucje odpowiedzialne za administrowanie adresami IP dla danych regionów świata. Lista nieprzydzielonych adresów IP jest ściśle strzeżoną tajemnicą, która nie powinna trafić w ręce cyberprzestępców.

NASK jako instytucja zarządzająca polską przestrzenią adresową IP, stale utrzymuje infrastrukturę darknet opracowaną i zbudowaną w ramach projektu SISSDEN[8]. System jest zintegrowany z platformami wymiany informacji o incydentach bezpieczeństwa (n6[9]) i aktywnie wykorzystywany

[5] https://www.nask.pl/
[6] Y. Liu, Improve DDoS botnet tracking with honeypots, https://www.botconf.eu/wp-content/uploads/2016/11/PR10-Improve-DDoS-Botnet-Tracking-WithHoneypots-LIU.pdf (dostęp: 17.01.2025).
[7] D. Moore, C. Shannon, G. M. Voelker, S. Savage, Network telescopes: Technical report, University of California, San Diego, Tech. Rep. 2004, s. 176.
[8] https://sissden.eu, Secure Information Sharing Sensor Delivery Event Network (SISSDEN)
[9] https://n6.cert.pl/

przez polski CERT[10], przy współpracy z organizacjami takimi jak Shadowserver[11]. Pomimo średniej rozdzielczości teleskopu sieciowego NASK (rozdzielczość odpowiada liczbie adresów IP monitorowanych przez teleskop - tu 250 tysięcy adresów IP), jest on na tyle „dokładny", że widoczne są w nim echa ataków DDoS.



Rysunek 1. Echo ataku DDoS (backscatter) przy spoofingu adresów IP obserwowane przez Teleskop Sieciowy.

Pojęcie echa ataku DDoS (ang. backscatter) ilustruje rysunek 1. Jest to zjawisko, będące efektem ataków DDoS, w których atakujący fałszuje (ang. spoofing) źródłowy adres IP w celu zmylenia ofiary i zatarcia śladów. Odpowiedzi ofiary na spreparowane pakiety trafiają więc w losowe miejsca, nierzadko w dużej liczbie na nieprzydzieloną przestrzeń adresów, gdzie mogą być zaobserwowane przez teleskop sieciowy. Dane z echa ataku DDoS pozwalają w pewnej mierze na odtworzenie i analizę ataków DDoS, a w efekcie dają szansę na określenie źródeł ataków, którym są zazwyczaj botnety. Informacje zaszyte są w nagłówkach rekonstruowanych pakietów i mogą one zostać wykorzystane do przygotowania sygnatur ataku.

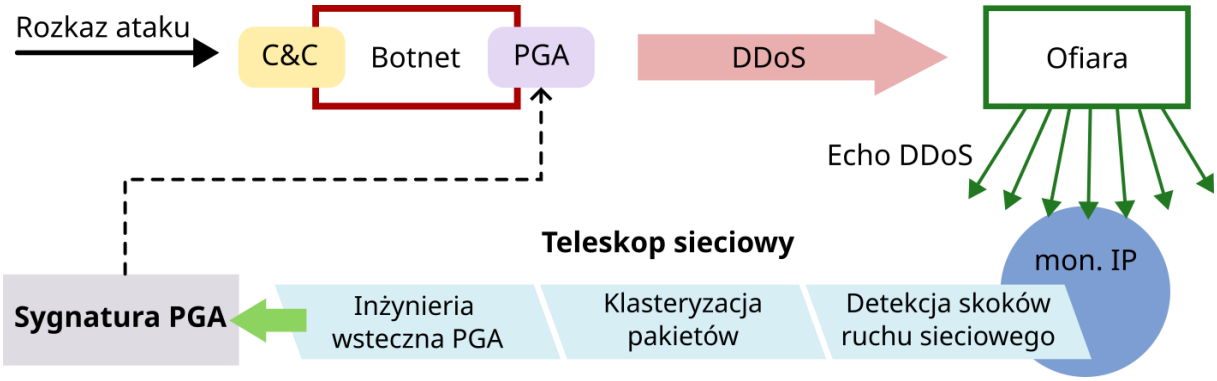
ALGORYTM GENEROWANIA PAKIETÓW (PGA)

Botnet może zostać zidentyfikowany na podstawie analizy złośliwego oprogramowania (ang. Command & Control) służącego do kontroli oraz przeprowadzania ataków z zainfekowanego komputera. W przypadku ataków DDoS skupiamy się na kodzie generującym ruch sieciowy. Procedura konstruowania złośliwych pakietów (ang. Packet Generation Algorithm - PGA) na przejętej maszynie zależy od rodzaju przeprowadzanego ataku. Często stosowana jest dodatkowa logika, która ma na celu przyspieszyć ten proces. Przyspieszenie osiągane jest przez optymalizację wykorzystania pamięci. Złośliwe pakiety tworzone dla wybranego profilu ataku powinny być dostatecznie różnorodne, aby nie dało się wykryć i zablokować ich prostą regułą firewall. Jednocześnie pola w nagłówkach pakietu muszą być poprawne, tzn. zgodne ze specyfikacją wykorzystywanych protokołów sieciowych. Zapewnienie różnorodności przez losowanie jest niewydajne ze względu na stosunkowo wysoki koszt obliczeniowy operacji losowania.

[10] https://cert.pl/
[11] https://shadowserver.org

Optymalizacją stosowaną w PGA jest ponowne wykorzystanie części zaalokowanej już pamięci do inicjalizacji kilku części nagłówka. Wartości są dodatkowo modyfikowane przez zastosowanie prostych operacji bitowych lub arytmetycznych w celu osiągnięcia pseudolosowości. Niska złożoność obliczeniowa ma tu kluczowe znaczenie. Sieci botnet najskuteczniej infekują urządzenia gorzej zabezpieczone, często są to starsze komputery czy sprzęt IoT, zwykle o mniejszej mocy obliczeniowej. Przyspieszenie algorytmu generowania pakietów nawet w niewielkim stopniu, przy odpowiednio dużej skali, przekłada się na znacznie większy wzrost wolumenu ruchu, zwiększając skuteczność ataku DDoS.

Implementacja PGA zależy od rodzaju ataku, ale także od wersji oprogramowania botnet. PGA może zatem służyć do zidentyfikowania konkretnych botnetów (ang. fingerprinting) na podstawie zebranych pakietów ataku.



Rysunek 2. Proces generowania nowej sygnatury PGA.

Echa ataków DDoS pozwalają w niektórych przypadkach na częściowe odtworzenie PGA. Proces generowania sygnatury ataku zilustrowano na rysunku 2.

Do wykrycia wzrostu liczby pakietów będących potencjalnym echem ataku stosowane są metody grupowania. Pakiety są grupowane względem czasu, adresów źródłowych, protokołów i innych parametrów wskazujących na ew. podobieństwo. Kolejnym krokiem jest próba częściowego odtworzenia nagłówków oryginalnych pakietów ataku. Proces inżynierii wstecznej (ang. reverse engineering) PGA polega na wyszukiwaniu powtarzających się zależności między polami nagłówków pakietów. Nawet częściowe odtworzenie algorytmu generowania pakietów pozwala przekształcić go w sygnaturę.

Przykładowa sygnatura PGA zapisana słownie może wyglądać następująco:

„Pierwsze dwa bajty (0, 1) ***ADRESU ŹRÓDŁOWEGO IP*** *jest równe pierwszym dwóm bajtom (0, 1)* ***NUMERU SEKWENCJI TCP*** *i ostatnie dwa bajty (2, 3)* ***ADRESU DOCELOWEGO*** *jest równe* ***NUMEROWI PORTU ŹRÓDŁOWEGO TCP”***

Zapisana w proponowanym przez autora skróconym formacie:

ip-src:0:1_is_tcp-seq:0:1_and_ip-dst:2:3_is_tcp-port-src

Powyższy przykład jest stosunkowo prostym przypadkiem PGA. W praktyce autorzy złośliwego oprogramowania korzystają z bardziej zaawansowanych metod uzyskiwania pseudolosowości i maskowania zależności między polami protokołu. Wykorzystują m.in. operacje bitowe takie jak: przesunięcia logiczne, negacje, inkrementację, dekrementację, itp. Oczywiście, zbyt skomplikowane operacje albo ich zbyt duża liczba, wydłużają czas generowania pakietu. Jest to zatem kompromis między wydajnością, a skomplikowaniem PGA w celu utrudnienia jego wykrycia.

Opisana procedura generowania sygnatur PGA jest zaimplementowana jako część półautomatycznego serwisu działającego w ramach Teleskopu Sieciowego NASK. Etap wstecznej inżynierii jest wspomagany wiedzą ekspercką. Algorytmy są wciąż udoskonalane, prowadzone są badania nad nowymi metodami zmierzające do pełnej automatyzacji procesu. Obecnie obsługiwane protokoły internetowe to: Ethernet, IPv4, IPv6, UDP, TCP, ICMP.

REALIZACJA MECHANIZMU WYKRYWANIA ATAKÓW DDoS

Skuteczne wykorzystanie sygnatur PGA do ochrony przed atakami DDoS wymaga wyspecjalizowanych narzędzi analizy ruchu. Sygnatury muszą być przetłumaczone na logikę, która zostanie wdrożona w infrastrukturze sieciowej chronionego systemu. Jednocześnie, efektywna mitygacja ataków DDoS wiąże się z koniecznością filtrowania dużych ilości danych o ruchu sieciowym w czasie rzeczywistym. Wydajność mechanizmów detekcji złośliwych pakietów jest kluczowa, aby skutecznie minimalizować wpływ ataku na działanie infrastruktury. Zbyt duże opóźnienia w przetwarzaniu pakietów mogą prowadzić do ograniczenia dostępności usług oraz potencjalnie zwiększać negatywne skutki ataku.

Aplikacja sygnatur PGA nie jest możliwa przy użyciu powszechnie wykorzystywanych rozwiązań. Systemy bazujące na sygnaturach ataku (Snort, Suricata), standardowe narzędzia filtrowania ruchu (iptables, nftables) oraz zapory sieciowe (firewalld, shorewall) nie wspierają natywnie kompletnego zbioru operacji występujących w sygnaturach PGA. Konieczne jest stworzenie dedykowanego rozwiązania.

Proponowana implementacja serwisu do filtrowania ruchu sieciowego za pomocą sygnatur PGA wykorzystuje technologię eBPF[12] (ang. extended Berkeley Packet Filter). Jest to mechanizm jądra systemu Linux, który w bardzo wydajny i elastyczny sposób umożliwia wykonywanie niskopoziomowych operacji filtrowania i przetwarzania pakietów sieciowych. W przeciwieństwie do tradycyjnych podejść niskopoziomowych, eBPF pozwala na dynamiczne ładowanie i uruchamianie kodu programowego bez konieczności modyfikowania jądra systemu operacyjnego. eBPF jest rozwiązaniem o otwartych źródłach (open-source), nie wymaga

[12] https://ebpf.io

specjalistycznego sprzętu sieciowego i może być wdrożony w każdej infrastrukturze Linux z aktualną wersją jądra.

Konwersja sygnatur PGA na kod wykonywalny jest możliwa, ponieważ eBPF, wspiera specjalny zestaw instrukcji, które pozwalają na implementację własnej logiki w języku programowania C (z pewnymi ograniczeniami). Każda sygnatura jest dynamicznie tłumaczona na kod, który weryfikuje, czy nagłówek sieciowy pasuje do wzorca sygnatury. Całość łączona jest w jeden program kompilowany do formatu eBPF bytecode. Program jest wykonywany w ramach jądra systemu Linux dla każdego przychodzącego pakietu sieciowego. Wczytanie nowego zbioru sygnatur wymaga ponownej kompilacji i podmiany obecnie działającej wersji programu. eBPF zapewnia atomowość tej operacji i ciągłość przetwarzania pakietów sieciowych bez opóźnień. Część serwisu działająca w tle zbiera statystyki dotyczące liczby pakietów pasujących do sygnatur.

PODSUMOWANIE

Krajobraz zagrożeń cybernetycznych podlega ciągłym zmianom wraz z rozwojem technologii informacyjnych i postępującą cyfrową globalizacją. Wzrost liczby urządzeń podłączonych do Internetu i rozwój infrastruktury sieciowej sprzyja ekspansji sieci botnet, co bezpośrednio przekłada się na coraz większy potencjał ataków cybernetycznych, w szczególności ataków DDoS. Potwierdzają to dane statystyczne[13], które jednoznacznie wskazują na narastający trend incydentów DDoS w sektorze prywatnym, przedsiębiorstwach państwowych i administracji państwa, jako formy nacisku i próby destabilizacji prowadzone w ramach konfliktów hybrydowych.

Wobec tak poważnego zagrożenia oczywistym krokiem powinno być podejmowanie wspólnych działań w celu skutecznego wykrywania i blokowania sieci botnet oraz ochrony przed atakami DDoS. W szczególności, sprawna wymiana informacji pozwoliłaby na skuteczniejszą walkę i ograniczenie zasięgu ataków. Podejście z wykorzystaniem sygnatur, będących spójnym zbiorem informacji o ataku, dobrze wpisuje się w taki scenariusz.

Prezentowane w artykule rozwiązanie to propozycja metody detekcji ataków DDoS za pomocą sygnatur sieci botnet, zaimplementowana z wykorzystaniem technologii jądra Linux. Oprogramowanie zostało wdrożone i przetestowane w projekcie europejskim GUARD[14] (ang. Guarantee Reliability and trust for Digital service chains), jako część modułu detekcji i mitygacji znanych zagrożeń sieciowych[15].

Bibliografia

Calleja A., Tapiador J., Caballero J., A Look into 30 Years of Malware Development from a Software Metrics Perspective, [in:] Research in Attacks, Intrusions and

[13] https://blog.cloudflare.com/tag/ddos-reports
[14] https://guard-project.eu/
[15] Szynkiewicz, P. (2022). Signature-Based Detection of Botnet DDoS Attacks. In: Kołodziej, J., Repetto, M., Duzha, A. (eds) Cybersecurity of Digital Service Chains. Lecture Notes in Computer Science, vol 13300. Springer, Cham. https://doi.org/10.1007/978-3-031-04036-8_6

Defenses. RAID Lecture Notes in Computer Science, Monrose F., Dacier M., Blanc G., Garcia-Alfaro J. [eds.], Springer Cham 2017, vol. 9854, https://doi.org/10.1007/978-3-319-45719-2_15

Dong S., Abbas K., Jain, R., A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. https://doi.org/10.1109/ACCESS.2019.2922196 (dostęp: 17.01.2025).

Brownlee N, One-way traffic monitoring with iatmon, [in:] Taft, N., Ricciato, F. (eds.) PAM 2012. LNCS, vol. 7192, pp. 179–188. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28537-0 18

C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.

D. Moore, C. Shannon, G. M. Voelker, and S. Savage, “Network telescopes: Technical report,” University of California, San Diego, Tech. Rep., 2004, https://www.caida.org/catalog/papers/2004 tr 2004 04/tr-2004-04.pdf

Silva, S.S., Silva, R.M., Pinto, R.C., Salles, R.M.: Botnets: a survey. botnet Activity: Analysis, Detection and Shutdown. Comput. Netw. 57(2), 378–403 (2013). https://doi.org/10.1016/j.comnet.2012.07.021, https://www.sciencedirect.com/science/article/pii/S1389128612003568

Liu, Y.: Improve DDoS botnet tracking with honeypots. https://www.botconf. eu/wp-content/uploads/2016/11/PR10-Improve-DDoS-Botnet-Tracking-WithHoneypots-LIU.pdf (2017).

Szynkiewicz, P. (2022). Signature-Based Detection of Botnet DDoS Attacks. In: Kołodziej, J., Repetto, M., Duzha, A. (eds) Cybersecurity of Digital Service Chains. Lecture Notes in Computer Science, vol 13300. Springer, Cham. https://doi.org/10.1007/978-3-031-04036-8_6

Detection and mitigation of botnet-generated DDoS attacks

Abstract

DDoS attacks (Distributed Denial of Service) pose a significant threat to network infrastructure and computer systems. Each year, there is observed growth in both the number and scale of attacks. The increasing potential of DDoS attacks is a consequence of the existence of extensive botnet networks, remotely controlled by cybercriminals, which serve as a tool for conducting such attacks. Therefore, continuous improvement of defensive mechanisms and the development of effective counter-strategies are necessary. The article presents a novel solution for detecting and mitigating DDoS attacks. The proposed method relies on attack signatures, an approach rarely used in the case of DDoS attacks. The signature generation procedure involves utilizing data acquired from the Network Telescope (darknet). An identification method (fingerprinting) of botnet-originating network packets is applied for this purpose. The idea behind, and the signature generation process is described and supported with an example. A general overview of the technologies used and the implementation approach of the presented method is provided.

Key words: cybersecurity, DDoS, signatures, Botnet.