SPIRIT VOL 16 NO 2 (2024) 358 - 365
JURNAL SPIRIT
225/E/KPT/2022

e-ISSN 2721-057X
p-ISSN 2085-3092

PENDETEKSI BOTNET MALWARE DDOS UNTUK MENCEGAH SERANGAN DISTRIBUTED DENIAL OF SERVICES

Slamet[1]
Prodi S1 Sistem Informasi [1] (Universitas Dinamika, Surabaya, Indonesia)
slamet@dinamika.ac.id

Naskah diterima: 1 Nopember 2024 ; Direvisi : 29 Nopember 2024 ; Disetujui : 30 Nopember 2024

Abstrak

Jaringan komputer berskala besar membutuhkan model deteksi dan respons yang efektif terhadap serangan DDoS. Berdasarkan kemajuan infrastruktur jaringan seperti server, switch, router atau peralatan jaringan lainnya, trafik serangan DDoS yang berasal dari sistem yang terinfeksi malware mampu melumpuhkan jaringan internal organisasi dan telah menjadi ancaman yang signifikan. Penelitian ini menghitung dan mencocokkan sejumlah atribut paket di dalam jaringan internal dan menganalisis atribut anomali sebagai pendeteksi serangan botnet Malware DDoS. Akurasi deteksi dan kinerja trafik yang dikumpulkan secara real time pada jaringan utama dianalisis menggunakan algoritma pendeteksi Botnet Malware DDoS. Hasilnya, serangan DDoS pada jaringan internal terdeteksi secara real time dengan banyaknya botnet DDoS yang tidak terkonfirmasi. Dengan mendeteksi host yang terinfeksi malware secara real-time, rencana tindak lanjut dapat dilakukan sebelum penghentian intrusi pada jaringan internal yang disebabkan oleh lalu lintas serangan DDoS berskala besar.

Kata kunci: Serangan DDoS, Deteksi, Botnet Malware

Abstract

Large-scale computer networks require an effective detection and response model for DDoS attacks. Based on the advancement of network infrastructure such as servers, switches, routers or other network equipment, DDoS attack traffic originating from malware-infected systems can paralyze an organization's internal network and has become a significant threat. This study calculates a number of packet attributes in the internal network and analyzes anomalous attributes to detect botnet Malware DDoS attacks. The detection accuracy and performance of real-time traffic collected on the core network are analyzed using the Botnet DDoS Malware detection algorithm. As a result, DDoS attacks on the internal network are detected in real time with many unconfirmed DDoS botnets. By detecting malware-infected hosts in real time, pre-termination responses to the internal network intrusion caused by large-scale DDoS attack traffic can be carried out.

Keywords: DDoS Attack, Detection, Botnet Malware

PENDAHULUAN

Kinerja peralatan pada infrastruktur jaringan komputer telah mengalami kemajuan yang sangat pesat [1] dengan banyaknya layanan informasi yang juga semakin canggih. Infrastruktur jaringan yang ada saat ini mampu mentransmisikan jutaan data [2] hanya dalam hitungan detik. Namun, di sisi lain bahwa sistem informasi yang mengalir pada infrastruktur jaringan justru lebih rentan [3] terhadap serangan siber yang disebabkan oleh malware.

Menurut [4], botnet malware berbasis Linux menyumbang proporsi tertinggi untuk serangan DDoS, dimana botnet tersebut menimbulkan ancaman besar terhadap layanan informasi perusahaan saat dipasang di perangkat-perangkat seperti access point, router, dan Network Attach Storage (NAS) [5].

Penelitian Akamai Technologies [6], malware XOR DDoS berbasis Linux mampu meluncurkan serangan DDoS hingga 350 Gbps, dan sistem yang terinfeksi malware mampu menyerang rata-rata 200 websites setiap hari. Untuk memasang dan menjalankan malware, penyerang memperoleh hak penuh dari sistem yang rentan dan menjalankan Command Shell [7] dengan memasang program malware yang berisi fungsi rootkit, sehingga memungkinkan penyerang juga menyembunyikan dirinya.

Penelitian-penelitian sebelumnya berfokus pada pendeteksian serangan DDoS dari internet ke dalam intranet [8] atau pendeteksian serangan dengan menganalisis informasi yang diambil dari agen botnet dalam sistem internal [9]. Akan tetapi, hanya sedikit penelitian yang membahas tentang pendeteksian serangan berbasis jaringan ketika jaringan internal berada dalam trafik DDoS dalam jumlah besar yang disebabkan oleh botnet malware DDoS atau infeksi lainnya. Jumlah besar ini, misalnya ketika serangan DDoS terjadi karena sistem yang terinfeksi malware di Server Zona Demiliterisasi (DMZ) dan banjir SYN terjadi di bagian jaringan dari sistem host ke sistem keamanan. Adanya keterbatasan sumber daya jaringan seperti bandwidth juga dapat mengganggu layanan jaringan.

Untuk itu, deteksi dan respons cepat terhadap sistem yang terinfeksi malware merupakan cara paling efektif untuk memastikan ketersediaan (availability) dari jaringan internal [9].

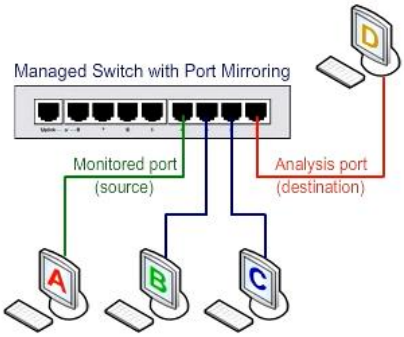
Penelitian ini mengimplementasikan algoritma Pendeteksi Botnet DDoS Malware untuk mendeteksi trafik anomali ketika host jaringan internal terinfeksi botnet dengan jumlah serangan yang besar. Algoritma pendeteksian mendapatkan pola dari informasi fitur botnet, dilanjutkan dengan menerapkan aturan pencocokan deteksi secara real time.

METODE PENELITIAN

Berdasarkan analisis trafik secara *real time*, penelitian ini mendeteksi sistem yang terinfeksi *Botnet* DDoS *malware*. Tahapan-tahapan untuk menyelesaikan penelitian dijelaskan dalam sub-bagian berikut.

1. Mengumpulkan Trafik Data dalam Jaringan

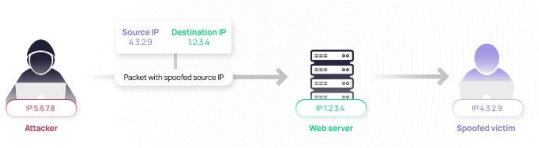
Untuk mengumpulkan trafik data secara terpusat digunakan salah satu *port* (misalnya *port 1*) di dalam Switch Layer 3 dengan teknik *port mirroring*. Salah satu *port* ini (*port* 1) adalah representasi jalur utama dari trafik data yang dilewati seluruh paket di dalam jaringan. Trafik ini dianalisis dan kemudian digunakan untuk mendeteksi infeksi *malware* serta mengidentifikasi sistem yang terinfeksi. Proses mengumpulkan data menggunakan teknik *port mirroring* dapat dilihat pada gambar 2. Sedangkan *bandwidth* layanan di jaringan yang diteliti, dibagi menjadi dua bagian yaitu *bandwidth* pengguna dan *bandwidth* server DMZ, sebagaimana terlihat pada topologi gambar 7.



Gambar 2. Proses Pengumpulan data menggunakan Teknik *port mirroring*

Sumber: https://www.miarec.com/legacy/what-is-port-mirroring

Diagram skematik untuk pengumpulan lalu lintas jaringan secara *real-time* dapat dilihat pada gambar 3.

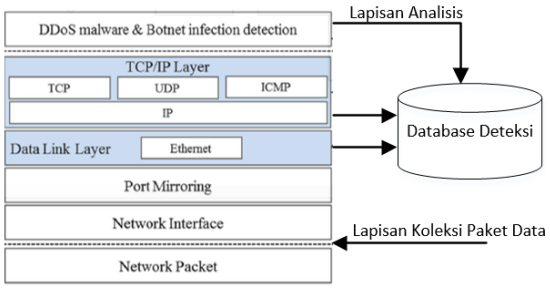


Gambar 3. Proses Deteksi DDoS di dalam jaringan

Sumber: https://sosafe-awareness.com/glossary/spoofing/

2. Ekstraksi paket data yang terkumpul

Seperti yang ditunjukkan pada Gambar 2, informasi atribut TCP/IP dan *header* Ethernet diekstraksi dari trafik yang dikumpulkan dan digunakan sebagai data dasar untuk menghasilkan *database* deteksi. Di dalam *database* ini terdapat tumpukan-tumpukan *protocol* yang kemudian diekstraksi menjadi informasi fitur.



Gambar 4. Tumpukan protokol untuk ekstraksi informasi fitur

Gambar 4 menunjukkan tumpukan protokol yang digunakan dalam mengekstraksi informasi fitur dari trafik secara *real time*. *Header* trafik yang mengalir

keluar dari jaringan internal digunakan untuk ekstraksi informasi fitur.

3. Membuat Tabel Deteksi

Tabel Deteksi digunakan untuk mendeteksi serangan DDoS dalam trafik secara *real time*, berisi nilai fitur yang berguna untuk mengidentifikasi sistem yang terinfeksi *malware*.

Prosedur untuk membuat tabel Deteksi adalah sebagai berikut:

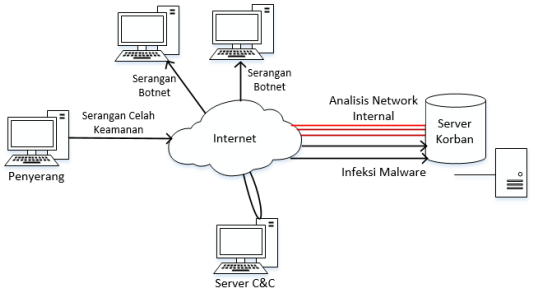
a. *Field* SN dari tabel deteksi menunjukkan urutan trafik dan *field* SGN, berarti jumlah grup yang terhubung ke IP tujuan yang sama.
b. Trafik *header* IP *Address* dan MAC *Address* diekstraksi dan disimpan dalam *field* SRC_IP, DST_IP, dan MAC untuk tabel deteksi. Protokol komunikasi antara dua *host* dan waktu akses juga disimpan.
c. *Field* TIN menunjukkan interval antara trafik sebelumnya dan trafik saat ini.
d. *Field* CND menunjukkan koneksi yang berhasil ke IP tujuan dan *field* RATD mewakili interval koneksi ulang IP tujuan.
e. *Field* STATE dikategorikan menjadi dua jenis. Jika nilai *field* TIN dan nilai RATD adalah nol dan *field* CNTI dibagi 180 d adalah ≤1 maka nilai *field* ditetapkan sebagai "abnormal". Sedangkkan semua yang lainnya ditetapkan sebagai "normal".

4. Analisis Informasi Fitur

Host yang terinfeksi *malware* menerima perintah serangan dari *server Command and Control* (C&C) atau membocorkan data penting ke *server C&C* [14]. Selain itu, *host* ini menerima perintah serangan DDoS dari *server* C&C atau menghasilkan trafik serangan Botnet DDoS berskala besar dalam waktu tertentu.

Melihat apa yang dialami *host* dan *bandwidth* jaringan, trafik DDoS yang dihasilkan saat ini dapat melumpuhkan jaringan internal dan membuatnya sangat sulit untuk mendeteksi *host* yang terinfeksi *botnet* DDoS *malware*.

Tabel deteksi yang ada digunakan untuk mendeteksi serangan DDoS, kemudian dilakukan analisis pada tabel ini [15] terkait waktu pembuatan dan frekuensi pembuatan trafik data, sehingga dapat ditentukan apakah serangan tersebut *botnet* yang menggunakan IP *Address* atau MAC *Address*. Untuk mendeteksi host yang terinfeksi *malware*, digunakan waktu koneksi kepada MAC *Address* dan IP *Address* tujuan serta frekuensi koneksi ke dua alamat ini. Gambar 5 menunjukkan tabel deteksi dengan hasil analisis dari informasi atribut trafik jaringan.

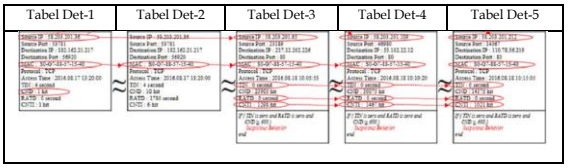


Gambar 5. Analisis informasi fitur menggunakan tabel deteksi

5. Deteksi serangan *Botnet DDoS Malware*

Untuk mendeteksi serangan *Botnet DDoS Malware* [16], dimulai dengan mengumpulkan informasi atribut dari jaringan inti kemudian dianalisis. Informasi atribut disimpan dalam tabel 2 dan informasi atribut relatif digunakan untuk mendeteksi serangan terlihat pada gambar 5.

Tabel 2. Tabel Deteksi dengan Anomaly Behaviour

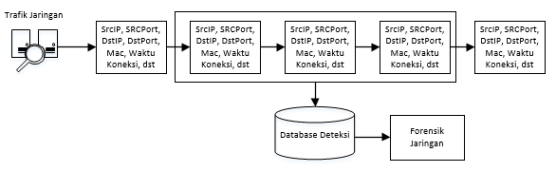


HASIL DAN PEMBAHASAN

Ketika serangan DDoS terjadi di jaringan internal, sistem yang menyusup harus dideteksi dan ditanggapi sebelum menghabiskan seluruh *bandwidth* jaringan internal. Selain itu, penyebab penyusupan harus dipahami dan audit jejak harus dilakukan untuk menghilangkan titik lemah yang ada.

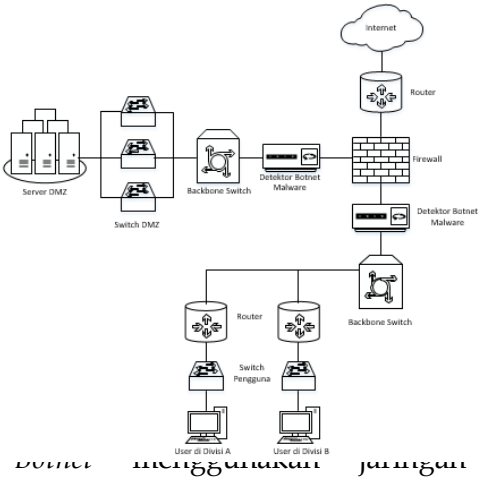
1. Forensik Jaringan

Untuk memahami arus trafik [17] dilakukan Forensik di dalam jaringan. Nilai atribut tabel deteksi digunakan untuk menganalisis sistem yang terinfeksi *malware* beserta kecenderungan serangan-serangannya. Gambar 6 adalah proses forensik jaringan menggunakan tabel deteksi.



Gambar 6. Forensik jaringan menggunakan tabel deteksi

Topologi pengujian sistem untuk mendeteksi serangan dan mengidentifikasi sistem yang terinfeksi *Botnet DDoS Malware*, dapat dilihat pada gambar 7.



em

ndeteksi

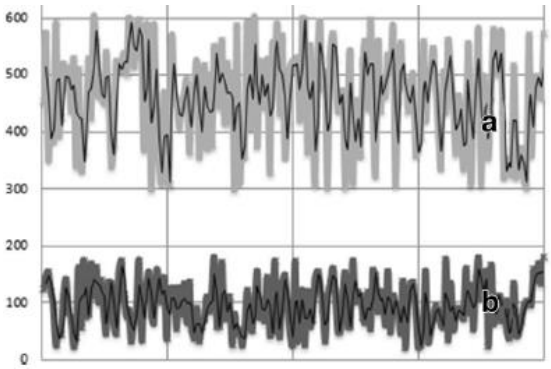
Botnet menggunakan jaringan Gigabit Ethernet dengan *DDOS Malware* yang dipasang di *server farm* jaringan DMZ. Spesifikasi komputer yang digunakan dalam pengujian adalah Prosesor Intel i7, RAM 16 GB, dengan HDD 2TB.

2. Hasil Deteksi dari *Botnet DDos Malware*

Tujuan dari penelitian ini adalah untuk mendeteksi dan merespons *malware* dengan cepat sebelum sumber daya jaringan habis ketika sejumlah serangan DDoS terjadi pada sistem yang terinfeksi *Botnet malware DDoS*. Hasil (waktu) pendeteksian serangan

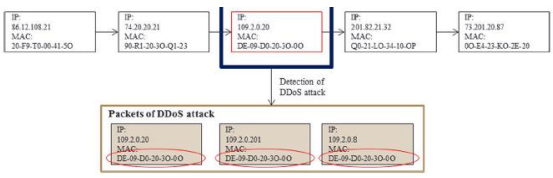
Botnet DDoS pada sistem yang terinfeksi *malware* ditunjukkan pada gambar 8.

Grafik A menunjukkan waktu terjadinya serangan *Botnet DDoS* karena *localhost* terinfeksi *malware*, sedangkan Grafik B adalah waktu ditemukan saat *localhost* terinfeksi *Botnet DDoS malware*. Waktu deteksi rata-rata untuk serangan *Botnet DDoS malware* pada *localhost* adalah 90 detik, sedangkan waktu terlama adalah 199 detik.



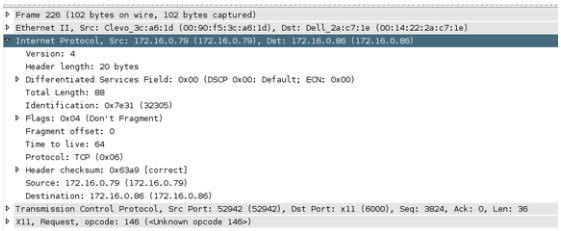
Gambar 8. Hasil Pengujian (waktu deteksi sistem yang terinfeksi oleh *malware*)

Gambar 9 menunjukkan mekanisme deteksi untuk serangan DDoS. Algoritma pendeteksian menganalisis *header* trafik secara *real time* untuk mendeteksi serangan *Botnet DDoS malware*.



Gambar 9. Mekanisme deteksi serangan DDoS

Gambar 10 menunjukkan informasi paket yang dikumpulkan oleh sistem pendeteksian. Waktu rata-rata yang dibutuhkan untuk mendeteksi sistem yang terinfeksi *Botnet DDoS malware* adalah 475 detik, sedangkan waktu terlama adalah 625 detik.



Gambar 10. Informasi paket yang dikumpulkan oleh Pendeteksian

KESIMPULAN

Penelitian ini menjelaskan penggunaan *Botnet DDoS malware* sebagai metode penyerangan, metode deteksi dan pencegahan serangan dalam jaringan. Serangan yang dilakukan mampu membuat koneksi dimana penyerang mendapatkan akses penuh kepada *host* dan menciptakan jalur masuk *backdoor* ke sistem korban. Sistem yang terinfeksi *botnet malware* DDoS mengakibatkan trafik DDoS dalam jumlah besar dan kebanjiran paket sehingga mempengaruhi komunikasi di jaringan internal.

Algoritma yang dihasilkan mampu mendeteksi serangan *Botnet DDoS malware* secara efektif dan mampu merespons sistem yang terinfeksi *malware* dengan cepat. Algoritma ini mendapatkan pola dari fitur *botnet* dan mencocokkan informasi dalam trafik *real time* dengan nilai properti tabel deteksi untuk

mendeteksi serangan *botnet DDoS malware* dan sistem yang terinfeksi *malware*.

DAFTAR PUSTAKA

[1] Farhatun Nisaul Ahadiyah, "Perkembangan Teknologi Infomasi Terhadap Peningkatan Bisnis Online," *INTERDISIPLIN: Journal of Qualitative and Quantitative Research*, vol. 1, no. 1, pp. 41–49, 2023, doi: 10.61166/interdisiplin.v1i1.5.

[2] J. F. Lempas and S. Soenarto, "Analysis of learning multimedia development needs for network infrastructure architecture," *IOP Conference Series: Materials Science and Engineering*, vol. 1098, no. 5, p. 052090, 2021, doi: 10.1088/1757-899x/1098/5/052090.

[3] A. Chernikova *et al.*, "Cyber Network Resilience Against Self-Propagating Malware Attacks," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13554 LNCS, no. 2019, pp. 531–550, 2022, doi: 10.1007/978-3-031-17140-6_26.

[4] O. Joy Sonia, U. Kingsley, and J. Sonia, "Analysis of Linux Kernel Iptables for Mitigating DDOS Attacks; A Component-Based Approach," *International Journal of Computer Science and Mathematical Theory*, vol. 9, no. September, pp. 10–21, 2023, doi: 10.56201/ijcsmt.v9.no4.2023.pg12.22.

[5] R. Sommese *et al.*, "Investigating the impact of DDoS attacks on DNS infrastructure," *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, pp. 51–64, 2022, doi: 10.1145/3517745.3561458.

[6] F. J. Ennemoser, P. Sattler, and J. Zirngibl, "State of the Art of DDoS Mitigation Techniques," 2022, doi: 10.2313/NET-2022-07-1.

[7] A. Bansal, D. Kapil, Anupriya, S. Agarwal, and V. Kumar Gupta, "Analysis and Detection of various DDoS attacks on Internet of Things Network," *International Journal of Wireless and Microwave Technologies*, vol. 12, no. 3, pp. 18–32, 2022, doi: 10.5815/ijwmt.2022.03.02.

[8] B. Tushir, Y. Dalal, B. Dezfouli, and Y. Liu, "A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6282–6292, 2021, doi: 10.1109/JIOT.2020.3026023.

[9] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, 2023, doi: 10.3390/jsan12040051.

[10] A. Singh and B. B. Gupta, "Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–43, 2022, doi: 10.4018/IJSWIS.297143.

[11] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149–171, 2021, doi: 10.1016/j.future.2021.03.011.

[12] S. Slamet, "Network Behavior Analysis (NBA) Untuk Mendeteksi Trafik Serangan Dalam Jaringan

Komputer," *SPIRIT*, vol. 15, no. 2, pp. 131–142, 2023.

[13] S. Sadrhaghighi, M. Dolati, M. Ghaderi, and A. Khonsari, "SoftTap: A Software-Defined TAP via Switch-Based Traffic Mirroring," *Proceedings of the 2021 IEEE Conference on Network Softwarization: Accelerating Network Softwarization in the Cognitive Age, NetSoft 2021*, pp. 303–311, 2021, doi: 10.1109/NetSoft51509.2021.9492588.

[14] S. Slamet, "Taksonomi Pertahanan Cyber Security Menggunakan Model Cyber Kill Chain," *Spirit*, vol. 16, no. 1, pp. 232–245, 2024, doi: 10.53567/spirit.v16i1.332.

[15] S. Bessid *et al.*, "Smart Ports Design Features Analysis : A Systematic Literature Review To cite this version : HAL Id : hal-03177580 Smart Ports Design Features Analysis : A Systematic Literature Review," 2021.

[16] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, "Performance evaluation of Botnet DDoS attack detection using machine learning," *Evolutionary Intelligence*, vol. 13, no. 2, pp. 283–294, 2020, doi: 10.1007/s12065-019-00310-w.

[17] A. V. Kachavimath, S. V. Nazare, and S. S. Akki, "Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics," *2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2020 - Conference Proceedings*, no. May, pp. 711–717, 2020, doi: 10.1109/ICIMIA48430.2020.9074929.