BOTNET DETECTION SURVEY

Adhitya Nugraha[1], Fauzi Adi Rafrastara[2]
Faculty of Information and Technology, University Teknikal Malaysia Melaka
adhitya_gro@yahoo.com[1] , fauzi_adi@yahoo.co.id[2]

ABSTRAK

Di antara berbagai bentuk malware, Botnet merupakan salah satu ancaman yang paling serius terhadap cyber-crime saat ini. Hal ini disebabkan karena Botnet mampu menyediakan platform yang dapat didistribusikan pada kegiatan ilegal seperti serangan-serangan di internet, termasuk spam, phishing, click fraud, pencurian password dan Distributed Denial of service(DDoS) attack.Akhir-akhir ini, deteksi Botnet telah menarik perhatian para peneliti untuk dijadikan topik penelitian dalam usaha pencegahan terhadap cyber-crime. Dalam paper ini, penulis melakukan studi literature untuk mengkaji beberapa penelitian sebelumnya yang membahas tentang teknik-teknik yang digunakan untuk mendeteksi keberadaan Botnet di dalam suatu sistem. Beberapa teknik yang dibahas dalam paper ini yaitu signature-based, anomaly-based, DNS-based, dan mining-base. Kajian komprehensif ini diharapkan dapat memberikan gambaran yang lebih jelas tentang teknik-teknik mendeteksi Botnet dengan memaparkan kelebihan dan kekurangan dari masing-masing metode tersebut yang selanjutnya dapat digunakan sebagai langkah awal dalam usaha prefentif terhadap serangan Botnet.

Kata kunci : *Botnet, deteksi Botnet, cyber-crime*

1. PENDAHULUAN

Internet dan aplikasinya seperti www dan email telah memberikan manfaat besar untuk kehidupan kita sehari-hari. Dalam penerapannya, internet sering kali digunakan untuk layanan penting seperti perbankan, bisnis, kedokteran, pendidikan, penelitian, perdagangan saham maupun peramalan cuaca. Hal ini memberikan dampak meningkatnya akses maupun pengiriman data berharga melalui internet.

Di sisi lain, hal ini dimanfaatkan oleh *user* jahat untuk mencuri informasi maupun data berharga dengan cara mengeksploitasi kelemahan dari sistem komputer maupun jaringan dengan menggunakan *malware* seperti *virus*, program *trojan, Botnet, worm* dan *spam mail* untuk memperoleh keuntungan pribadi.

Di antara berbagai bentuk *malware*, *Botnet* merupakan salah satu ancaman yang paling serius terhadap *cyber-crime* saat ini. *Botnet* merupakan kumpulan dari aplikasi *bot* (robot) yang di*setting* untuk dapat berjalan otomatis dalam suatu jaringan. Tiap komputer yang telah terinfeksi dan tergabung dalam jaringan *Botnet* akan menjalankan perintah atau instruksi yang diberikan oleh *Botmaster* yang dilakukan secara *remote*.

Studi menunjukkan bahwa infeksi *Botnet* terhadap komputer ditahun 2010 memiliki jumlah dua kali lipat daripada tahun sebelumnya dimana dalam kurun waktu setengah tahun, microsoft telah menemukan 6.5 juta komputer diseluruh dunia yang terinfeksi oleh *Botnet* [1]. Hal ini menunjukan bahwa *Botnet* adalah amcaman serius bagi dunia *cyber*.

Di awal paper ini, penjelasan singkat tentang peranan dan ancaman *Botnet* telah dipaparkan. Selanjutnya, sisa materi dari paper ini disusun sebagai berikut. Bagian II menggambarkan pengenalan tentang *Botnet*. Pada bagian ini, karakteristik *Botnet* dan siklus hidup *Botnet* dijelaskan untuk memberikan pemahaman yang lebih baik terhadap *Botnet*. Bagian III membahas teknik-teknik dalam mendeteksi *Botnet*. Dalam bagian ini, empat kelas pendekatan dalam deteksi *Botnet* yaitu *signature-based, anomaly-based, DNS-based* dan *mining-based* akan dibahas secara terpisah. Kesimpulan dari paper ini dipaparkan dibagian IV.

2. PENGENALAN BOTNET

Botnet menjadi salah satu ancaman paling serius terhadap keamanan internet. Hal ini disebabkan karena *Botnet* mampu menyediakan *platform* yang dapat didistribusikan pada kegiatan ilegal seperti serangan-

serangan di internet, termasuk *spam, phishing, click fraud,* pencurian *password* dan *Distributed Denial of Service(DDoS) attack*[2,3,5].

Salah satu kemampuan dari *Botnet* yang membedakannya dari *malware* yang lain adalah *Botnet* dapat dikendalikan dari jauh oleh seseorang (*Botmaster*) dibawah suatu infrastruktur yang disebut *Command and Control (C & C) channel*. *Host* yang terinfeksi *malware* ini, atau biasa disebut *bot*, tidak secara fisik dimiliki oleh *Botmaster* dan mungkin terletak di beberapa lokasi yang mencakup seluruh dunia [2,4]. Perbedaan zona waktu, bahasa, dan hukum inilah yang membuat sulit melacak keberadaan dan aktivitas berbahaya dari *Botnet*. Karakteristik ini membuat *Botnet* menjadi alat yang menarik untuk kejahatan dan bahkan menimbulkan ancaman besar terhadap *cyber-security*. Dalam rangka untuk memberikan pemahaman yang lebih baik tentang fenomena *Botnet*, karakteristik *Botnet* dan siklus hidup *Botnet* akan dijelaskan secara masing-masing.

2.1 Karakteristik Botnet

Seperti *malware* lainnya, *Botnet* adalah perangkat lunak yang dirancang untuk masuk atau merusak sistem komputer tanpa sepengetahuan pemilik. Hal ini dilakukan dengan cara memanfaatkan dan menginfeksi kelemahan suatu sistem dari sebuah *host*, kemudian mengeksploitasi kinerja dari sistem tersebut untuk keperluan pribadi ataupun memperluas jangkauan mereka.

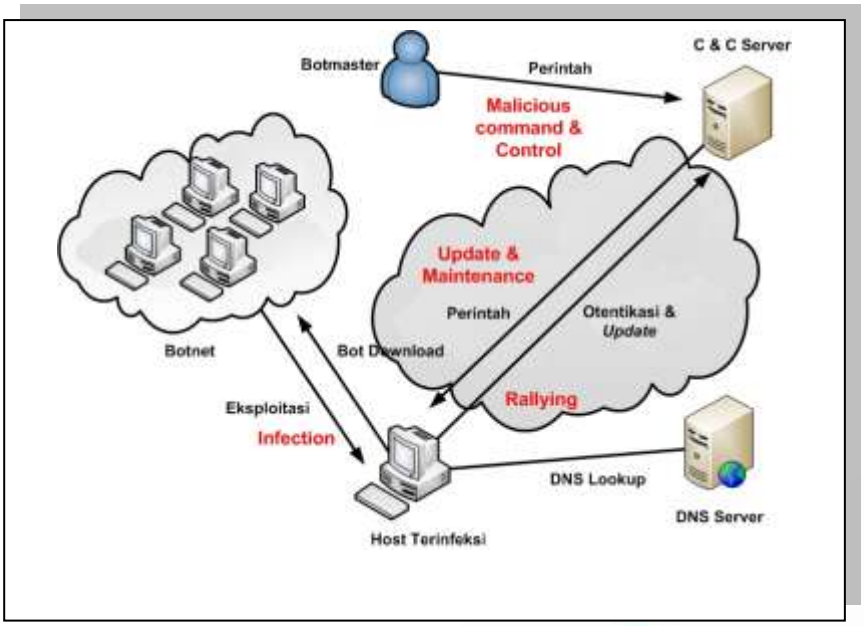
Perbedaan utama antara *Botnet* dan jenis *malware* lainnya adalah adanya infrastruktur *Command-and-Control (C & C)*. *C & C* memungkinkan sejumlah bot untuk dapat menerima perintah untuk melakukan *update* atau bahkan malakukan kejahatan seperti *DDOS attack, spaming* dan lainnya sebagaimana yang diinginkan oleh *Botmaster* [2,3,4,5].

Generasi pertama dari *Botnet* adalah *centralized C & C model* yang memanfaatkan *IRC (Internet Relay Chat)* protokol sebagai jalur komunikasi antara *C & C server* dan bot [2,3,4]. IRC protokol pada awalnya dirancang untuk komunikasi satu ke banyak (*one to many*). Hal ini dimanfaatkan *Botmaster* untuk mengontrol bot dalam jumlah banyak untuk memaksimalkan keuntungan mereka. Dalam implementasinya, C*entralized C & C model* memberikan kemudahan bagi *Botmaster*. Namun, C*entralized C & C model* membuat *Botnet* menjadi lebih rentan saat dideteksi sehingga mudah menemukan *C & C server* untuk kemudian menghancurkannya. Contoh *Botnet* ini adalah AgoBot, SDBot dan Zotob[3].

Dikarenakan adanya kelemahan dari C*entralized C & C model* ini, kemudian diciptakan *Botnet* generasi baru yang dapat menyembunyikan komunikasi *Botnet* dengan *C & C server*, yang disebut *Peer-to-Peer (P2P) model* [2,3,4]. Dibandingkan dengan *Centralized C & C model, P2P model* jauh lebih sulit untuk ditemukan dan dihancurkan. Karena sistem komunikasi tidak sangat bergantung pada server tertentu saja. Menghancurkan satu atau bahkan sejumlah bot, tidak akan menyebabkan kerusakan dari seluruh *Botnet*. Beberapa *bot* seperti Phatbot dan Peacomm telah menggunakan komunikasi P2P sebagai alat untuk mengontrol *Botnet* [3].

2.2 Siklus Hidup Botnet

Dalam penyebarannya, *Botnet* memiliki siklus hidup yang terdiri dari 4 tahap, yaitu: *infection, rallying, malicious command and control, update and maintenance.*



Gambar 1: Siklus Hidup *Botnet*

Bot mampu mendistribusikan dirinya sendiri melalui jaringan internet dengan mencari celah terhadap komputer yang rentan dan tidak dilindungi agar dapat diinfeksi. *Malware* ini umumnya disebar oleh para *Botmaster* dengan menyusupkannya ke situs-situs legal yang telah dieksploitasi; instalasi software dari sumber yang tidak dipercaya; mengirimkan *spam mail* untuk memperdaya korban sehingga mengklik *link* tertentu; dan *backdoor* yang ditinggalkan oleh *virus* [2,4].

Setelah fase *infection* sukses, *host* yang terinfeksi akan mendownload *script code bot* dari sebuah *remote server* dan diinstal secara otomatis yang kemudian merubah host tersebut menjadi "zombie". Meskipun urutan siklus hidup kadang dapat bervariasi, di beberapa titik awal siklus hidup klien *Botnet* yang baru harus melaporkan diri ke "rumah" (C & C server), proses ini disebut *rallying.*

Proses *rallying* diawali dengan proses pencarian *C & C server* oleh *host* baru yang terinfeksi dengan menggunakan *DNS lookup*. Kebanyakan *Botnet* menggunakan *Internet Relay Chat (IRC) server* sebagai *C & C server* untuk mengontrol *Botnet* mereka. Setelah mendapatkan alamat *C & C server*, *bot* kemudian melakukan *login* dan mengotentikasikan dirinya sebagai bagian dari *Botnet* tertentu. Pada titik ini, *Botmaster* dapat mengeluarkan perintah kepada bot untuk melakukan serangan seperti *spamming, click fraud, DDoS attack* ataupun menyebarkan *malware* untuk memperluas jaringan mereka. Hal ini yang disebut *malicious command and control*.

Disisi lain, *Botmaster* dapat melakukan perintah *update* terhadap bot untuk melakukan pembaruan dengan cara mendownload *script code* yang baru untuk beberapa alasan seperti menambah fungsionalitas *bot army*, menghindari pendeteksian, atau memperbaharui alamat *C & C server*. Ini akan menjamin bahwa *bot* dapat dikelola dan dapat diamankan dari pendeteksian. *Bot* tetap tersembunyi sampai mereka diinformasikan oleh *Botmaster* untuk melakukan serangan atau tugas.

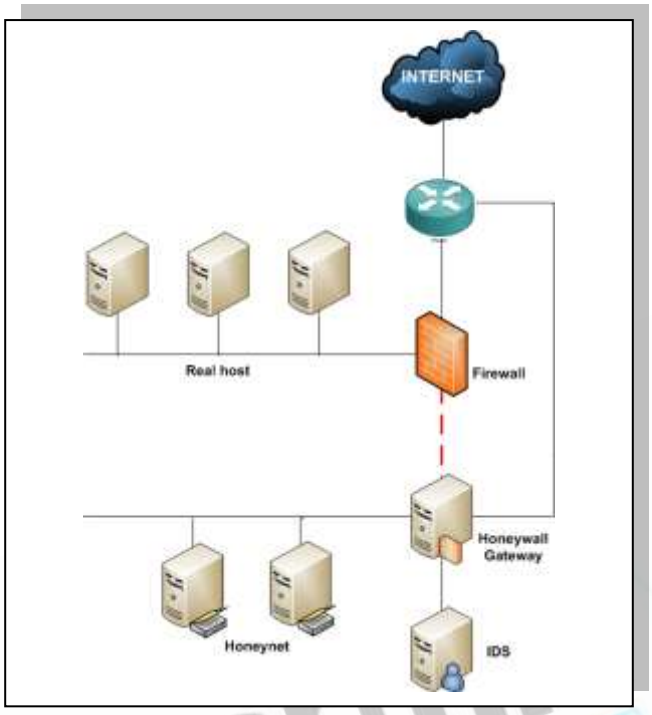
3. TEKNIK DETEKSI BOTNET

Ada dua pendekatan utama dalam deteksi *Botnet* yaitu dengan metode yang berdasarkan *Honeynet* dan didasarkan pada p*assive network monitoring.*

3.1 Honeynet

Honeynet merupakan suatu jaringan yang terdiri dari satu *honeypot* ataupun lebih. Sedangkan *honeypot* sendiri adalah perangkap yang bertindak sebagai umpan untuk memikat *client* yang berpotensi sebagai penyerang yang mecoba masuk secara paksa ke dalam suatu sistem. *Honeypot* digunakan untuk memantau dan mempelajari metode yang digunakan *hacker* untuk menembus suatu sistem. Informasi yang didapatkan akan digunakan sebagai tindakan prefentif dimasa mendatang [3,6].

Umumnya *honeypot* terdiri dari komputer, data, dan segmen jaringan yang terlihat seperti bagian dari suatu jaringan utuh yang dirancang untuk meniru sistem yang ada. Tapi ternyata segmen jaringan *honeypot* itu terisolasi. Kebanyakan *honeypot* terinstal di dalam *firewall* sehingga mereka dapat dikendalikan lebih baik, namun ada kemungkinan bagi mereka untuk diinstal dari luar firewall. Untuk menambah daya tarik bagi penyerang, biasanya honeypot terlihat seolah-olah berisi informasi atau sumber data yang akan bernilai bagi penyerang dan dikonfigurasi sedemikian rupa sehingga menjadi sistem yang sangat *vulnerable*.



Gambar 2: Arsitektur Honeynet

Honeypot memiliki fitur monitoring untuk memantau aktivitas penyerang ketika masuk ke dalam sistem *honeypot*. Aktivitas yang bisa diketahui diantaranya *port* yang diserang, *command* yang diketik oleh penyerang, perubahan yang dilakukan penyerang di server palsu *honeypot*, dsb. Hal ini dapat dimanfaatkan oleh *Network Administrator* sebagai masukan untuk *patch* ke sistem asli, melakukan konfigurasi di segmen jaringan asli untuk dilakukan pencegahan dini, dan sebagainya.

Seperti yang dijelaskan dalam paper [3,6], honeypot dapat digunakan sebagai sistem untuk mencegah maupun mendeteksi keberadaan *Botnet*. Sistem ini juga mampu membantu mengamati dan mendeteksi keberadaan orang yang menjalankan *Botnet* atau biasa disebut dengan *Botmaster*.

3.2 Passive network monitoring

Pendekatan lain untuk deteksi *Botnet* dilakukan melalui pendekatan *passive network monitoring* dengan pertimbangan *honeynet* tidak selalu mampu mendeteksi infeksi yang dilakukan *Botnet* setiap waktu. Teknik ini dilakukan dengan memonitor lalu lintas yang melewati suatu jaringan dan kemudian dilakukan analisis untuk mengidentifikasi keberadaan dan memahami karakteristik *Botnet*. Teknik ini dapat diklasifikasikan menjadi *signature-based*, *anomaly-based*, *DNS-based*, dan *mining-based* yang akan dijelaskan pada bagian dibawah ini.

3.2.1 *Signature-based Detection*

Sebuah *Intrusion Detection system (IDS)* biasanya diletakan di tempat yang strategis pada suatu jaringan untuk memindai paket masuk dan keluar yang ada pada jaringan tersebut sekaligus menganalisanya. IDS sendiri adalah sebuah aplikasi perangkat lunak atau perangkat keras yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan di dalam sebuah sistem jaringan.

Teknik *signature-based* mengidentifikasi paket yang melewati suatu jaringan dan kemudian mencocokannya dengan informasi-informasi yang diperoleh dari penelitian yang sebelumnya. Bagian paket yang diteliti dapat berupa *signature*, perilaku maupun ukuran dari paket. Dalam hal ini, *signature* adalah kode ataupun perilaku yang secara unik mengidentifikasikan *Botnet* tertentu. Kelemahan dari teknik ini adalah tidak dapat diterapkan untuk mendeteksi *Botnet* yang belum diketahui.

Dalam paper [7], Sunny et al., mengusulkan sebuah mekanisme *Network-based Detection and Prevention System (N-EDPS)* sebagai tindakan pendeteksian dan pencegahan *Botnet*. Sebuah pendekatan baru juga diperkenalkan dalam paper ini yang disebut *extrusion detection system* untuk mengenali pola-pola paket dari *host* terinfeksi yang melewati jaringan. Berbeda hal dengan i*ntrusion detection system* yang digunakan untuk mendeteksi anomali jaringan yang masuk kedalam sistem. Informasi dari *extrusion detection* ini yang digunakan untuk mengupdate dari sistem deteksi yang ada. Metode ini menunjukan hasil yang baik saat pendeteksian tetapi tidak dapat digunakan untuk mendeteksi *C & C channel* yang terenkripsi, ataupun menemukan *C & C server*.

3.2.2 *Anomaly-based Detection*

Anomaly-based detection melakukan pendekatan untuk mendeteksi *Botnet* berdasarkan pada beberapa anomali lalu lintas jaringan seperti latensi jaringan yang tinggi, volume lalu lintas yang tinggi, lalu lintas yang tidak biasa di *port*, dan perilaku sistem yang tidak biasa yang dapat mengindikasikan potensi ancaman adanya *bot* berbahaya dalam jaringan.

Pendeteksian model ini didasarkan pada perubahan dalam pola pemakaian atau kelakuan sistem. Hal pertama yang dilakukan adalah membangun sebuah model statistik yang berisi satuan-satuan ukuran yang nilainya akan diambil dari aktifitas proses sistem untuk membangun deksripsi yang merepresentasikan penggunaan atau pola perilaku normal.

Kemudian, teknik statistik digunakan untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Hal ini dapat ditempuh melalui penghitungan nilai rata-rata dan standar deviasi dari statistik lalu listas jaringan. Jika hasil perhitungan berada diluar dari parameter standar deviasi, maka ini mengindikasikan kemungkinan perilaku tidak normal. Selanjutnya, deskripsi atau pola ini dibandingkan dengan perilaku sistem untuk memprediksi dan mendeteksi ketidakcocokan yang mungkin timbul. Sehingga pada akhirnya akan dikenali kemungkinan adanya bot berbahaya dalam jaringan.

Pada tahun 2007, Karasaridis et al. [8], mengembangkan algoritma analisis pasif berbasis anomali yang mampu mendeteksi *controller IRC Botnet* pada *layer transport* tanpa perlu untuk mengetahui *signature* atau binari. Algoritma ini juga mampu mendeteksi komunikasi *Botnet* yang terenkripsi, membantu mengidentifikasi dan mengkarakterisasi kegiatan *Botnet* dalam jaringan. Sama halnya dengan Zilong et al. [9], mengembangkan *framework* untuk mendeteksi anomali dari sebuah jaringan berdasarkan IRC protokol di level Gbit/s. Akan tetapi, metode ini tidak dapat diterapkan untuk protokol non-IRC. Sedangkan Gu et al. [10], telah mengusulkan Botsniffer yang menggunakan *anomaly-based detection* untuk mengidentifikasi *Botnet C & C channel* dalam *local area network* tanpa perlu pengetahuan sebelumnya dari *signature* ataupun lokasi C & C server. Pendekatan deteksi dapat mengidentifikasi baik server C & C dan host yang terinfeksi dalam jaringan.

3.2.3 *DNS-based Detection*

DNS-based Detection dilakukan berdasarkan informasi DNS yang dihasilkan oleh sebuah *Botnet*. Teknik *DNS-based* mirip dengan teknik *anomaly-based* sebagaimana menerapkan algoritma deteksi anomali untuk diterapkan pada deteksi DNS. Seperti disebutkan sebelumnya, *bot* biasanya melakukan koneksi dengan *C & C* server untuk mendapatkan perintah ataupun *update*. Untuk mengakses *C & C server, bot* melakukan query DNS untuk menemukan lokasi *C & C* server. Jadi, sangatlah memungkinkan untuk mendeteksi *Botnet* dengan memonitor dan mendeteksi lalu lintas DNS.

Pada tahun 2007, Choi et al. [11] mengusulkan sebuah mekanisme untuk mendeteksi anomali *Botnet* melalui pemantauan lalu lintas DNS, yang membentuk *group activity* dalam DNS query secara simultan yang dikirim oleh bot. Pada fase *rallying*, kebanyakan *Botnet* menggunakan DNS untuk menemukan C & C server. Dari fase ini, para peneliti telah mendefinisikan fitur unik dari lalu lintas domain sebagai *group activity* untuk membedakan query DNS *Botnet* dari query DNS yang sah. Mereka juga mengembangkan mekanisme yang memungkinkan untuk mendeteksi migrasi C & C server. Mekanisme deteksi ini

menunjukan hasil yang lebih baik daripada pendekatan sebelumnya dan dapat mendeteksi *Botnet* baik yang sudah diketahui maupun yang belum diketahui, hanya dengan melihat *group activity* mereka di lalu lintas DNS. Namun demikian, kekurangan utama dari pendekatan ini adalah waktu pemrosesan yang tinggi yang diperlukan untuk memonitor jaringan skala besar.

3.2.4 *Mining-based Detection*

Salah satu manfaat besar IDS adalah mekanisme yang mampu merekam kejadian dalam sistem, kemudian mengauditnya hingga dapat menginformasikan jika terjadi aktifitas mencurigakan dalam lalu lintas jaringan. Mengingat besarnya volume data yang akan di audit, baik itu disebabkan oleh data yang terlalu banyak, maupun banyaknya bagian dari sistem yang akan dianalisa, maka dibutuhkan sebuah tools untuk melakukan analisa data secara efisien dan cerdas.

Istilah *data mining* digunakan untuk menjelaskan proses penggalian informasi tersembunyi untuk mencari pola atau informasi menarik dengan menggunakan teknik atau metode tertentu didalam suatu basis data yang besar. Teknik data mining juga dapat digunakan untuk mendeteksi *Botnet* seperti yang dijelaskan pada paper [12]. Beberapa teknik data mining termasuk *classification, link analysis* dan *sequence analysis* dapat membuat pendeteksian *Botnet* maupun *C & C server* menjadi lebih efisien.

Data mining umumnya mengacu pada model proses otomatisasi untuk pengauditan data dalam jumlah besar. Perkembangan dalam proses data mining telah diterapkan untuk algoritm pada *machine learning, pattern recognition machine* dan lainnya. Keuntungan utama dari pendekatan ini adalah bahwa penggalian informasi terhadap kumpulan data yang besar dapat dilakukan secara otomatis untuk dapat menghasilkan model deteksi ringkas dan akurat. Tujuan utama dari teknik ini adalah untuk mendeteksi penyebaran *Botnet* dan menemukan *C & C server* berdasarkan *logfiles* yang telah dikumpulkan.

M. Masud et al. [13] mengusulkan deteksi *Botnet* yang akurat dan efektif terhadap dua *logfiles* yang masing-masing dihasilkan oleh *tcpdump* dan *exedump*. *Tcpdump* akan merekam semua paket yang dikirim ataupun yang diterima oleh *host*, sedangkan *exedump* akan merekam aplikasi yang dieksekusi oleh *host*. Mereka memperkenalkan deteksi trafik C & C terhadap dua *logfiles* ini yang kemudian mengklasifikasikan seluruh aliran paket untuk mengidentifikasi *C & C server* dari *Botnet*. Metode ini lebih bersifat general karena tidak memberikan batasan apapun terhadap protokol komunikasi *Botnet*, sehingga metode ini juga berlaku untuk *Botnet* non-IRC.

4. KESIMPULAN

Botnet merupakan ancaman yang serius untuk perkembangan *cyber-crime* saat ini. Hal ini dikarenakan *Botnet* mampu menyediakan *platform* untuk didistribusikan pada kegiatan ilegal seperti serangan-serangan di internet, termasuk *spam, phishing,* click fraud, pencurian password dan *Distributed Denial of service(DDoS) attack*. Meskipun telah banyak akibat buruk yang ditimbulkan oleh *Botnet*, namun hanya sedikit studi formal yang membahas secara detil tentang penelitian *Botnet*.

Seperti yang disebutkan dalam paper ini, hal yang membedakan *Botnet* dengan *malware* lainnya adalah adanya infrastruktur *Command-and-Control (C & C)* yang memungkinkan *Botnet* dapat menerima perintah dari *Botmaster*. Hal inilah yang membuat penelitian tentang *Botnet* menjadi tugas yang sangat menantang.

Dalam paper ini, kami telah membahas teknik-teknik yang saat ini digunakan untuk mendeteksi *Botnet*. Survey ini mengklasifikasikan teknik deteksi *Botnet* menjadi dua kategori utama, yaitu: honeynet dan *passive network monitoring.* Selanjutnya, kami membagi *passive network monitoring* menjadi beberapa kategori, yang terdiri atas: *signature-based, anomaly-based, DNS-based, dan mining-base.* Pengenalan dan penelitian terkait juga telah disampaikan pada setiap pembahasannya, untuk mendukung kebenaran dalam paper ini.

DAFTAR PUSTAKA

[1] http://www.pcpro.co.uk/news/security/361876/microsoft-*Botnet*-infections-double-globally
[2] Saha B, Gairola A. "Botnet: An Overview." *CERT-In White Paper, CIWP-2005-05*. 2005.
[3] Bacher P, Holz T, Kotter M, Wicherski G. "Know your enemy: Tracking Botnets." *The Honeynet Project*. 2005:1-21.

[4] Zhu Z, Lu G, Chen Y, et al. "*Botnet* Research Survey." *32nd Annual IEEE International Computer Software and Applications Conference*. 2008:967-972.
[5] Micro T. "Taxonomy of Botnet threats." *Trend Micro White Paper, Tech. Rep*. 2006;(November):1-15.
[6] Wang P, Wu L, Cunningham R, Zou CC. "Honeypot detection in advanced Botnet attacks." *International Journal of Information and Computer Security*. 2010;4(1):30.
[7] Behal S, Brar AS, Kumar K. "Signature-based Botnet Detection and Prevention." *rimtengg.com.* 2010.
[8] Karasaridis A, Rexroad B, Hoeflin D. "Wide-scale Botnet detection and characterization." *In: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets. USENIX Association*; 2007:7–7.
[9] Zilong W, Jinsong W, Wenyi H, Chengyi X. "The Detection of IRC Botnet Based on Abnormal Behavior." *Second International Conference on Multimedia and Information Technology*. 2010:146-149.
[10] Gu G, Zhang J, Lee W. BotSniffer: "Detecting Botnet command and control channels in network traffic." *In: Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08). Citeseer*; 2008.
[11] Choi H, Lee H, Lee H, Kim H. "Botnet Detection by Monitoring Group Activities in DNS Traffic." *7th IEEE International Conference on Computer and Information Technology* (CIT 2007). 2007:715-720.
[12] Thuraisingham B, Khan L, Masud MM, Hamlen KW. "Data Mining for Security Applications." *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.* 2008:585-589.
[13] Masud M, Al-khateeb T, Khan L, Thuraisingham B, Hamlen K. "Flow-based identification of Botnet traffic by mining multiple log files." *In: Distributed Framework and Applications*. *First International Conference on. IEEE*; 2008:200–206.