Analisis dan Implementasi *Honeypot* Terdistribusi sebagai Deteksi Aktivitas *Blackhat* pada Jaringan

Setio Wahono[1], Alif Subardono[2]
Program Studi DIV Teknologi Jaringan
Sekolah Vokasi, Universitas Gadjah Mada
Yogyakarta, Indonesia
[1]setiowahono@gmail.com, [2]alif@ugm.ac.id

***Abstrak*—Keamanan sistem komputer yang secara langsung terkoneksi ke internet menjadi semakin penting setiap harinya karena penggunaan ribuan komputer yang dikompromikan secara intensif mencari kelemahan pada sistem komputer dapat berujung pada serangan yang sukses. Agar mampu mempelajari motif, taktik, dan alat yang sekarang banyak digunakan oleh komunitas *blackhat,* sistem *honeypot* dapat dengan mudah dimanfaatkan untuk tujuan tersebut. Makalah ini memuat analisis dan implementasi beberapa sensor Dionaea yang diintegrasikan menggunakan Hpfeeds pada sistem MHN (*Modern Honey Network*) dalam jaringan internet kampus Universitas Gadjah Mada untuk menemukan aktivitas *blackhat* berupa pola dan *cluster* serangan terhadap network *services* serta *malware* sebagai informasi terhadap administrator.**

Kata Kunci—honeypot; Dionaea; pola serangan; malware

I. PENDAHULUAN

Keamanan sistem komputer yang secara langsung terkoneksi ke internet menjadi semakin penting setiap harinya karena penggunaan ribuan komputer yang dikompromikan secara intensif mencari kelemahan pada sistem komputer dapat berujung pada serangan yang sukses. Agar mampu mempelajari motif, taktik, dan alat yang sekarang banyak digunakan oleh para penyerang, sistem *honeypot* dapat dengan mudah dimanfaatkan untuk tujuan tersebut. *Honeypot* sendiri adalah sistem terkontrol yang sengaja dipasang sehingga mampu berinteraksi dengan penyerang di dalam jaringan untuk mengumpulkan data serangan, teknik, dan perilaku serangan komunitas *blackhat* [7]. Perangkat keamanan lainnya seperti IDS konvensional hanya dapat mengatasi serangan berdasarkan *signature*, dimana penyerang dapat melewati *signature check* menggunakan pola aliran berbeda dengan serangan yang sama berbahayanya. Oleh karena itu *honeypot* menjadi sangat berguna untuk mengumpulkan data serangan yang belum diketahui.

Honeypot menjebak serangan *hacker* dan *malware*, mencatat informasi intrusi tentang metode dan aktivitas proses *hacking* serta mencegah serangan keluar dari lingkungan sistem yang terganggu. Karena nilai berharga *honeypot* berasal dari penggunaan sumber daya yang tidak sah dan kemampuan beberapa *honeypot* seperti Dionaea yang dapat mencatat segala informasi mengenai serangan yang ditangkap dan salinan berkas *binary malware* [1]. *Honeypot* yang yang secara individual difungsikan sebagai sensor sekaligus penyimpanan data serangan pada jaringan internet UGM telah diimplementasikan sebelumnya menggunakan PC desktop [6]. Setelah berjalan beberapa tahun dan menyimpan banyak data di dalamnya, terlihat penurunan performa yang dialami oleh sistem *honeypot* Dionaea tersebut.

Pemasangan *honeypot* Dionaea secara tradisional pada mikrokomputer seperti Raspberry Pi dalam jaringan dapat menyebabkan permasalahan karena ia hanya mempunyai *resource* dan *storage* yang terbatas menjadikannya tidak memungkinkan untuk menyimpan seluruh data serangan [1]. Terlebih lagi jika terdapat banyak individual sensor *honeypot* yang berdiri sendiri tanpa adanya supervisi, data yang tersimpan di dalam mesin *honeypot* masing-masing akan sukar untuk digabungkan dan dinormalkan sehingga mempersulit proses analisis serangan. Dibutuhkan perangkat yang mampu menampung semua *log* serangan setiap *honeypot* yang terhubung ke data *collector*. Maka dari itu penelitian ini menggunakan Hpfeeds pada MHN (*Moden Honey Network*) untuk mengalirkan *realtime attack events* dari sensor Dionaea menuju *server* penampung MongoDB. Sensor-sensor *honeypot* yang terpasang pada Raspberry Pi hanya difungsikan sebagai deteksi sehingga mengurangi beban kerja mesin *honeypot* untuk tidak menampung seluruh data serangan pada dirinya sendiri.

Penelitian ini menggunakan beberapa sensor *honeypot* Dionaea untuk merekam aktivitas penyerang dan mengumpulkan *malware* mulai Juli 2016 sampai dengan Juli 2017 di jaringan internet Universitas Gadjah Mada. Analisis data memperlihatkan aktivitas alamat IP paling tinggi, *port* yang paling banyak diserang, dan jenis *malware* yang kerap menginfeksi di jaringan. Dengan hasil informasi yang didapatkan administrator mampu melakukan tindakan pencegahan terhadap jaringan atau perangkat yang sebenarnya.

II. HONEYPOT SEBAGAI PENDETEKSI DAN LOGGER AKTIVITAS BLACKHAT

Blackhat merupakan orang-orang yang melanggar etika keamanan komputer karena alasan sepele atau untuk keuntungan pribadi. Bentuk *hacker* ini menulis program untuk merusak sistem komputer dan jaringan [9].

Berbagai ancaman berbahaya yang dapat ditimbulkan oleh komunitas *blackhat* diantaranya adalah DDoS (*Distributed Denial of Service*) karena mampu menurunkan atau mengganggu layanan pengguna yang sah dengan menghabiskan sumber daya komunikasi, komputasi dan atau memori dari target melalui volume paket yang besar [3], juga infeksi *malware*, *virus*, *worm* dan sebagainya. Sebelum serangan-serangan tersebut diluncurkan, *blackhat* akan mencari informasi terlebih dahulu mengenai target sasaran dan membuat profil mereka, fase ini biasa disebut *footprinting* [8]. Setelah fase *footprinting*, *blackhat* akan mencari saluran komunikasi yang terbuka pada sistem dengan melakukan serangan terhadap *port*. Dengan *port scanning*, penyerang dapat mencari informasi mengenai sistem target: apa yang dijalankan pada layanan, apa yang pengguna miliki pada *service* tersebut, apakah *login* secara anonim diijinkan, dan apakah layanan pada jaringan membutuhkan otentikasi. *Port scan* menunjukkan bahwa ada kemungkinan terjadinya serangan dalam waktu dekat. *Port scanning* sama seperti mengetuk pintu dan menentukan apa yang sistem dengarkan dan dicapai lewat internet [6]. Komunitas *blackhat* yang telah mengetahui kerentanan jalan masuk yang terbuka menuju sistem target sudah dipastikan akan segera melancarkan aksi serangan selanjutnya. Sehingga dengan menganalisis *port scanning attacks* dapat memberikan informasi mengenai prediksi serangan selanjutnya di dalam sistem.

Infeksi *malware* dilakukan setelah menemukan saluran komunikasi layanan *vulnerable* yang dapat dimanfaatkan untuk membuka saluran komunikasi ilegal lain (*backdoor*) untuk mendapatkan akses yang tidak sah. Virus, *worm*, dan trojan *horse* komputer diklasifikasikan sebagai *malware* atau *malicious software*, yaitu program-program yang bertindak tanpa sepengetahuan pengguna dan seenaknya mengubah operasi-operasi komputer. Pemrogram yang jahat menulis *malware* kemudian mengujinya untuk meyakinkan bahwa *malware* buatannya dapat mengirimkan *payload*-nya. *Payload* merupakan kejadian atau trik destruktif yang ingin dikirimkan oleh program [10].

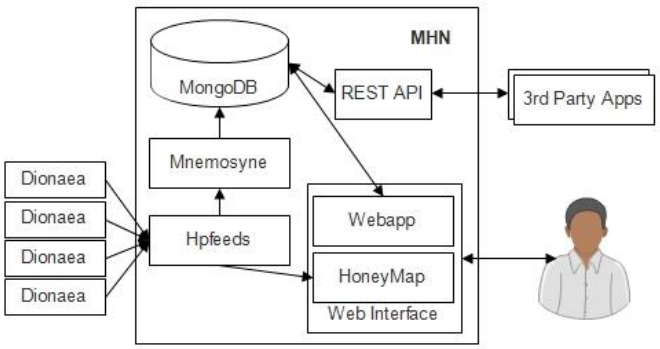
Malware yang aktif dapat mempunyai banyak varian baru. Para pembuat *malware* terus berusaha untuk mencari lubang keamanan atau sistem yang *vulnerable* sebagai target serangan *malware* yang mereka buat. Sistem yang selalu mendapat pembaruan resmi sekalipun memungkinkan untuk terjangkit *malware*. *Malware* dengan jenis yang sama dapat dibungkus dengan *pack* yang berbeda untuk mengelabui *antivirus* sehingga menganggapnya sebagai berkas yang legal dan sukses menginfeksi sistem target.

Honeypot adalah *security resource* yang yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan [5]. Pada umumnya *honeypot* berupa komputer, data, atau situs jaringan yang terlihat seperti bagian dari jaringan, tapi sebenarnya terisolasi dan dimonitor. Jika dilihat dari kacamata komunitas *blackhat* yang akan menyerang, *honeypot* terlihat seperti layaknya sistem yang patut dan mudah untuk diserang.

Honeypot Dionaea merupakan salah satu jenis *low-interaction honeypot* yang sengaja ditaruh dengan pengamanan minimal agar mudah diserang *blackhat* dan disusupi segala jenis *malware*. Dionaea merupakan penerus dari *honeypot* sebelumnya, yakni Nepenthes. Menggunakan python sebagai bahasa pemrogramannya, dan libemu sebagai pendeteksi *shell code*. Dionaea adalah jenis *honeypot* yang dapat memberikan layanan jaringan yang nantinya dapat dieksploitasi. Tujuan dari Dionaea adalah untuk mendapatkan salinan dari *malware* yang telah dikirim oleh penyerang, sehingga seorang administrator dapat memutuskan sesuatu untuk melindungi sistem induk, bahkan menciptakan antivirus baru. Menurut Markus Koetter, salah satu pengembang Dionaea [4], *low-interaction honeypot* Dionaea mampu menjebak *malware* melalui emulasi beberapa layanan diantaranya SMB, HTTP, HTTPS, FTP, TFTP, MSSQL, dan VoIP.

III. HONEYPOT TERDISTRIBUSI

MHN (*Modern Honey Network*) Merupakan proyek yang dikembangkan oleh Anomali [2]. MHN hanya dapat mengintegrasikan dan mengelola *low-interaction* serta *medium-interaction honeypot*. Ia tidak dapat memasang *high-interaction honeypot* yang memang membutuhkan infrastruktur kompleks untuk mengamankannya. Dengan *server* terpusat dan alat untuk mengelola *honeypot*, MHN didesain untuk dapat dipasang pada jaringan *honeypot* terdistribusi yang besar. Arsitektur sistem MHN ditunjukkan pada Gambar 1.



Gambar 1. Arsitektur sistem MHN

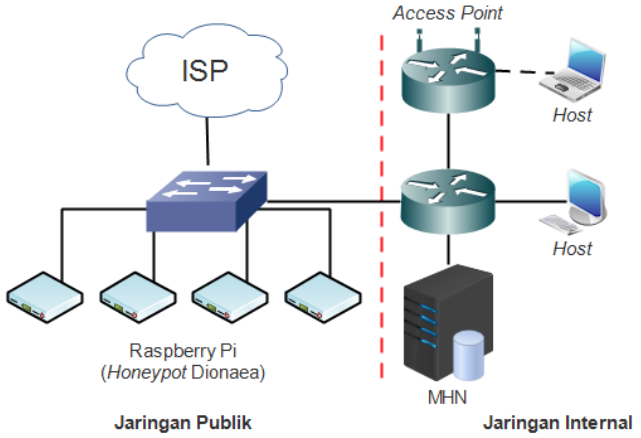
Honeypot Dionaea tradisional akan menyimpan *log* serangannya di dalam *file* sqlite secara lokal. Hal ini tentu memberatkan kerja mikrokomputer Raspberry Pi yang berbekal kartu *microsd* sebagai *storage* utamanya. Maka dari itu, hpfeeds berperan penting dalam mendistribusikan *event* serangan secara *realtime* kepada MHN, kemudian disimpan dalam *repository* penyimpanan pusat MongoDB. Data dinormalisasikan via Mnemosyne agar memungkinkan analisis sensor agnostik.

Data serangan diekspos melalui RESTful API. Serangan secara *realtime* divisualisasikan pada Honeymap dengan membaca *live stream* hpfeeds. Honeymap juga mampu untuk menampilkan *geolocation* pada peta dunia berformat SVG untuk merepresentasikan lokasi asal dan target serangan pada saat itu juga.

IV. METODOLOGI DAN PERCOBAAN

A. Topologi Jaringan

Gambar 2. menunjukkan rancangan topologi jaringan yang digunakan untuk mengimplementasikan beberapa sensor *honeypot* Dionaea pada MHN di jaringan internet kampus UGM. sensor *honeypot* dionaea diletakkan pada jaringan publik bersama dengan *server* lain sehingga dapat diakses lewat internet dan berinteraksi dengan komunitas *blackhat*. Sedangkan *server* MHN sebagai kolektor akan ditempatkan di jaringan internal sehingga hanya dapat di-*remote* dari jaringan lokal UGM.



Gambar 2. Topologi jaringan

B. Prosedur Penelitian

Prosedur penelitian diawali dengan pemasangan MHN pada jaringan lokal, kemudian mengintegrasikan sensor *honeypot* dionaea pada jaringan publik dengan alamat IP xxx.yyy.92.50, xxx.yyy.92.54, xxx.yyy.93.210, dan xxx.yyy.93.214. Dengan mengintegrasikan sensor-sensor ini pada MHN, maka secara otomatis sensor tidak akan menyimpan data serangan di dalam *local storage* karena telah didistribusikan menuju *repository* utama dalam MHN menggunakan hpfeeds.

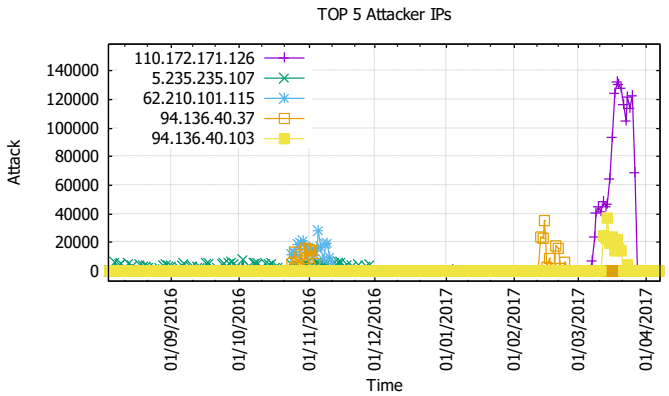
Penelitian dilakukan dengan mengekstraksi data *honeypot* pada MongoDB di dalam MHN yang telah beroperasi selama hampir 1 tahun mulai dari 13 Juli 2016 sampai 06 Juli 2017. Informasi yang diekstrak di antaranya adalah alamat IP penyerang, *port* target, *network service* target, *timestamp* dan *hash malware*. Alamat IP *blackhat* yang paling sering menyerang akan digali informasi pentingnya mengenai siapa dia dengan melakukan pencarian pada beberapa situs penyedia *blacklist*, serta kapan ia aktif menyerang. Berikutnya, *clustering* serangan *port* ditujukan untuk mencari suatu *port network services* yang pernah diserang sebelumnya, lantas dicari hitungan serangnya serta *hit* alamat IP yang pernah menyerang dirinya. *Clustering* digunakan untuk mengetahui *port* manakah yang memiliki *vulnerability* paling tinggi dan paling kerap menjadi target sasaran para *blackhat*. Pemisahan dilakukan dengan mencari tahu tingkat ketertarikan penyerangan ataukan rendah, sedang, atau tinggi berdasarkan perhitungan menggunakan algoritma K-*means clustering*. Terakhir, tipe dan varian *malware* didapatkan berdasarkan penamaan terbanyak oleh *antivirus* yang terintegrasi Virustotal.

V. HASIL DAN PEMBAHASAN

Hasil penelitian yang dilakukan dengan memasang beberapa sensor *honeypot* selama hampir 1 tahun di jaringan internet UGM memperlihatkan pemakaian *resource* yang lebih ringan pada sensor jika dibandingkan dengan sensor honeypot Dionaea tradisional. Penelitian ini juga berhasil mengumpulkan total 19.586.493 serangan, 736.341 alamat IP unik, dan 1.159 *hash* unik. Setelah melakukan ekstraksi dan *query* aggregasi pada *repository* utama, didapatkan informasi terkait serangan yang ditujukan terhadap sensor *honeypot* Dionaea diantaranya:

A. Alamat IP dengan Percobaan Serangan Terbanyak

Gambar 3. menampilkan pola distribusi serangan dari 5 alamat IP teratas.



Gambar 3. Pola serangan 5 alamat IP teratas

Posisi pertama penyerang terbanyak ialah alamat IP 110.172.171.126. Alamat IP ini mempunyai reputasi yang buruk setelah dilakukan pengecekan reputasi IP melalui salah satu *tools* pada web https://www.whatismyip.com/blacklist-check/. IP ini juga ter-*blacklist* oleh JustSpam.org, inps.de-DNSBL, juga Barracuda *Reputation Block List*. Ia berasal dari kota Coimbatore, India. Alamat IP ini mulai aktif menyerang pada tanggal 20/12/2016, kemudian hanya terlihat beberapa kali di bulan Janurai dan Februari 2017. Baru di bulan Maret 2017 dirinya terlihat melancarkan serangan besar dari tanggal 08/03/2017 sampai dengan 27/03/2017 hingga mencapai rata-rata 81.000 lebih serangan perharinya pada saat itu seperti terlihat pada pola grafik yang naik sangat tajam di bulan Maret 2017 untuk alamat IP ini.

Di awal kemunculannya pada tanggal 06/08/2016, alamat IP 5.235.235.107 menyerang 2 kali pada *port* 445. Selanjutnya, mulai tanggal 07/08/2016 sampai dengan 29/11/2016 secara intensif alamat IP ini terus menyerang dengan rata-rata perharinya mencapai 3.300 lebih serangan secara konstan sehingga dimungkinkan bahwa alamat IP ini dikendalikan oleh *bot*. Meskipun begitu, serangan paling tinggi yang dilakukan terjadi pada tanggal 03/10/2016 mencapai 7.682 serangan. Tentu saja alamat IP ini mempunyai reputasi yang buruk sehingga masuk ke dalam daftar *blacklist* di antaranya oleh JustSpam.org dan McAfee RBL. Alamat IP ini dimiliki oleh

organisasi *Telecommunication Company of* Gilan, di negara Iran.

Alamat 62.210.101.115 tergabung dalam blok alamat IP 62.210.0.0/16 yang dimiliki oleh ISP bernama ONLINE S.A.S. yang bertempat di Fontenay-aux-Roses, Perancis. IP ini muncul pertama kali pada tanggal 25/10/2016 kemudian tidak terlihat lagi setelah tanggal 12/11/2016. Selama itu pula, ia terus menyerang *honeypot* Dionaea hingga rata-rata perharinya sebesar 15.100 lebih serangan. Serangan paling tinggi terjadi pada tanggal 06/11/2016 menyentuh angka 28.453 dan lebih besar dibanding alamat IP sebelumnya. Ini membuktikan bahwa alamat IP ini menyerang dengan frekuensi serangan lebih besar dan padat dalam jangka waktu hanya 19 hari.

Alamat IP 94.136.40.37 merupakan salah satu alamat yang dimiliki oleh ISP Host Europe GmbH di negara Inggris. Ia terlihat di tanggal 25/10/2016 hingga 04/11/2016 kemudian tidak melakukan aktivitas penyerangan pada bulan Desember maupun Januari. Tetapi ia kembali menampakkan diri pada bulan Februari yakni tanggal 13/02/2017 setelah itu tidak terlihat lihat lagi setelah tanggal 24/02/2017. Rata-rata serangan perharinya dapat mencapai 11.700 lebih, sedangkan serangan paling tinggi yang ia lancarkan terjadi pada tanggal 15/02/2017 sebesar 35.174 mengalahkan alamat IP sebelumnya yang hanya mencapat 28 ribu. Alamat IP ini juga mempunyai reputasi yang lumayan buruk sehingga mendapatkan *blacklist* oleh JustSpam.org dan SpamCannibal.

Terakhir adalah IP dengan alamat yang masih satu blok dengan alamat IP sebelumnya yaitu 94.136.40.103 milik *Host* Europe GmbH. Alamat IP ini hanya muncul untuk menyerang di tanggal 13/02/2017 sampai dengan tanggal 24/02/2017 dan setelahnya tak terlihat lagi. Rata-rata serangan perhari yang dilakukan olehnya yakni sebesar 19.900 lebih serangan. Sedangkan serangan tertinggi terjadi pada tanggal 15/02/2017, sebesar 37.307 yang mana melampaui serangan tertinggi IP sebelumnya. Namun tidak seperti alamat IP sebelumnya, alamat IP ini terlihat berbeda. Ia tidak ter-*blacklist* oleh https://www.whatismyip.com/blacklist-check/.

B. Clustering Serangan Port Terhadap Network Services

Tabel 1. menunjukkan hasil dari beberapa *clustering* serangan *port* teratas.

TABEL I. HASIL *CLUSTERING* SERANGAN *PORT* TERATAS

***Hit* Dionaea**	**Kontribusi Serangan (%)**	**Nomor *Port***	***Hit* IP**
3.493.303	38,05%	445	26.766
1.258.397	13,71%	5060	3.582
979.151	10,67%	23	528.032
567.903	6,19%	139	17.550
454.265	4,95%	3306	6.904

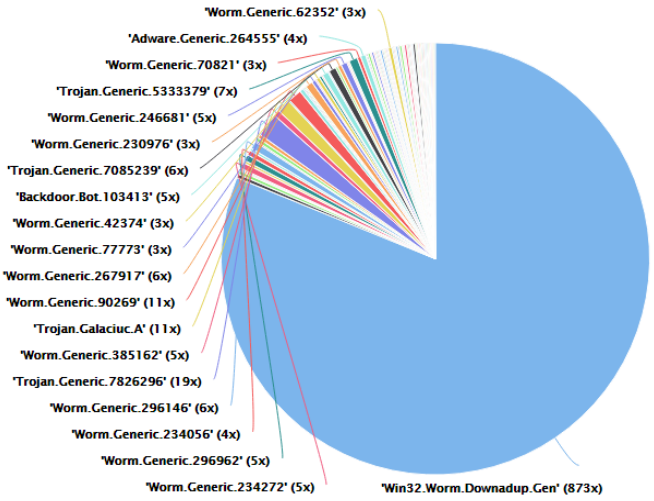
Urutan target serang teratas adalah *port* nomor 445 yang menjalankan layanan SMB yakni *port* 445 dengan jumlah penyerang 26.766 beralamat IP unik dan total serangan sebesar 3.493.303 kali. Layanan SMB juga mempunyai sejarah yang cukup banyak berkaitan dengan *remote exploitable bug*. Maka dari itu, protokol ini menjadi target favorit *blackhat* untuk menginfeksi jaringan dengan *worm*. Terlihat bahwa *malware* yang paling kerap menginfeksi, *worm* umumnya menempati urutan pertama karena memang terdapat celah keamanan dalam *port* 445 *honeypot* yang menjadi target serang komunitas *blackhat*. Target serang terbesar kedua adalah *port* 5060 yang menjalankan layanan VoIP dengan jumlah penyerang unik hanya sebesar 3.582 tetapi dengan jumlah total yang besar yakni 1.258.397 kali serangan. Berikutnya adalah *port* 23 dan 139 dengan masing-masing total serangan 979.151 dan 567.903. Mereka menjalankan layanan yang sama yaitu pcap. Terakhir layanan yang paling diserang adalah mysqld yang berjalan pada *port* 3306 dengan jumlah total 454.265 serangan.

C. Malware yang Paling Banyak Menginfeksi

Gambar 5. menunjukkan jenis *malware* yang paling kerap menginfeksi jaringan. Dari 1.159 *unique hash*, dapat dikelompokkan menjadi beberapa *malware* dengan kemiripan nama setelah diidentifikasi menggunakan Virustotal. Pada penelitian ini, dominasi *malware* yang berhasil diunduh, 83% teridentifikasi sebagai *worm*. Jumlah paling banyak yakni 873 *hash* dikenali sebagai Win32.Worm.Downadup.Gen. *Worm* jenis ini mengekploitasi *vulnerability* Windows. Ia juga memanfaatkan *network shares* dan *password* yang lemah, serta memanfaatkan *autorun* Windows untuk menggandakan dirinya. Trojan juga ditemukan pada penelitian ini. Sistem berhasil mengidentifikasi sebesar 5,61% *malware* adalah trojan. Sisanya dengan jumlah sedikit diidentifikasi sebagai *generic malware*, virus, *adware*, dan lainnya seperti yang tertera pada Tabel 2. Sayangnya, sebanyak 83 *hash* tidak dapat diidentifikasi atau tidak terdapat pada *database* Virustotal sehingga tidak dapat diketahui jenisnya.

TABEL II. TIPE DAN VARIAN MALWARE YANG TERIDENTIFIKASI

Tipe Malware	**Jumlah Varian**	**Jumlah *Download***	**Presentase**
Worm	40	972	83,87%
Trojan	21	65	5,61%
Generic Malware	17	17	1,46%
Backdoor	5	10	0,86%
Virus	4	8	0,69%
Adware	1	4	0,35%
Unknown	-	83	7,56%



Gambar 5. Malware yang paling kerap menginfeksi

VI. KESIMPULAN

Dengan mengintegrasikan sensor-sensor *honeypot* dionaea ke dalam MHN, bebankerja yang dilakukan oleh sensor menjadi lebih ringan dibandingkan dengan pemasangan *honeypot* Dionaea secara tradisional. Analisis data juga dapat dilakukan secara terpusat dan terkelola dengan efisien karena data *log* telah dinormalkan kemudian ditampung dalam satu lokasi yakni MongoDB.

Pola serangan yang diperlihatkan oleh setiap alamat IP berbeda-beda karena setiap *blackhat* mempunyai tujuan dan target serangnya masing-masing. Berbeda halnya dengan pola serangan yang ditunjukkan oleh *bot. Bot* dapat diprogram untuk terus-menerus melakukan serangan atau *scanning* pada targetnya dalam durasi yang lama juga dengan porsi serangan yang telah ditentukan seperti serangan yang dilakukan oleh alamat IP 5.235.235.107.

Port 445 merupakan *port* terfavorit sebagai target serangan di jaringan internet Universitas Gadjah Mada karena *port* yang menjalankan layanan SMB ini sudah dari dulu mempunyai banyak masalah yang berkaitan dengan *exploit* secara *remote* dalam *file sharing*, sehingga protokol ini kerap digunakan sebagai media untuk menyebarkan *worm* di jaringan. Terbukti *malware* yang berhasil diunduh oleh *honeypot* Dionaea, sebesar 83,87% diidentifikasi sebagai tipe *worm* yang memanfaatkan celah pada layanan ini.

DAFTAR PUSTAKA

[1] Charles Lim, Mario Marcello, Andrew Japar, Joshua Tommy, I Eng Kho, "Development of Distributed Honeypot Using Raspberry Pi", International Conference on Information, Communication Technology and System (ICTS), pp. 233-236, September 2014.

[2] MHN, http://threatstream.github.io/mhn/ [Diakses: 25 April 2017].

[3] Paul Bächer, Thorsten Holz, Markus Kötter, Georg Wicherski, “Know your enemy: Tracking botnets”, Honeynet.org. 08 September 2008, [Online]. Tersedia: http://www.honeynet.org/papers/bots/ [Diakses: 18 April 2017].

[4] Dionaea, https://github.com/rep/dionaea [Diakses: 25 April 2017].

[5] Firrar Utdirartatmo, Trik menjebak hacker dengan honeypot. Yogyakarta : ANDI, 2005.

[6] Raditya Aji Habsoro, Nur Rohman Rosyid, Hidayat Nur Isnianto, "Implementasi Honeypot untuk Mengungkap Pola Port Scanning Attacks dalam Jaringan", 7th National Conference on Information Technology and Electrical Engineering (CITEE), pp. 139-143, September 2015.

[7] Brijendra Pal Singh, C. Rama Krishna, Rakesh Sehgal, Sanjeev Kumar "Implementation of Port Density Based Dynamic Clustering Algorithm on Honeynet Data", International Journal of Advanced Computational Engineering and Networking ISSN: 2320-2106, Volume 2, Issue-6, pp. 76-82, Juni 2014.

[8] Honeynet Project, Know Your Enemy: Learning about Security Threats. Addison Wesley Press, 2001.

[9] Robert Moore, Cybercrime: Investigating High-Technology Computer Crime. Abingdon : Routledge, 2010.

[10] Gary B. Shelly, Thomas J. Cashman, Misty E. Vermaat, Jeffrey J., Discovering Computers: Fundamentals. Toronto : Thompson, 2006.