IMPLEMENTASI MONITORING AUTONOMOUS SPREADING MALWARE DI ITS-NET DENGAN DIONAEA DAN CUCKOO

Febrian Bramanta Alfiansyah, Bambang Setiawan, S.Kom, M.T, Bekti Cahyo Hidayanto, S.Si, M.Kom
Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111
E-mail: febrianba@gmail.com, setiawan@is.its.ac.id, bekticahyo@is.its.ac.id

***Abstrak*— Akhir tahun 2013 Indonesia berada di posisi teratas sebagai Negara dengan *traffic malware* tertinggi. Hal ini membuat miris, Indonesia yang pengguna internetnya baru seperempat dari total populasi bisa menciptakan masalah *malware* sedemikian besar. ITS (Institut Teknologi Sepuluh Nopember) sebagai perguruan tinggi yang mengedepankan teknologi informasi patut mempertimbangkan masalah *malware* ini. Kebutuhan akan *traffic* informasi yang tinggi membuat seluruh sistem harus handal dan tersedia setiap kali pengguna ingin mengaksesnya. Pada penelitian ini dilakukan implementasi *Honeypot Dionaea dan Cuckoo* di infrastuktur ITS-Net untuk memonitor *autonomous spreading malware*. Monitoring dilakukan untuk mengetahui jenis dan persebaran *malware* yang ada di lingkungan jaringan ITS-Net. Dari penelitian ini *Honeypot Dionaea* mendapatkan jumlah serangan sebanyak 322537 kali dalam kurun waktu 4 bulan. Jumlah binaries malware unik yang berhasil didapatkan sebanyak 362. Dari 10 sampel *autonomous spreading malware* yang diidentifikasi dengan *Sanbox Cuckoo* ditemukan jenis Trojan sebanyak 40%, Worm sebanyak 30%, Botnet sebanyak 20% dan Spyware sebanyak 10%.**

Kata kunci: Malware, Honeynet, Kemanan Komputer, Honeypot Dionaea, Cuckoo

I. PENDAHULUAN

Selama evolusi teknologi komputer, pertumbuhan penggunaan internet terus meningkat sampai sekarang. Berdasarkan statistik penggunaan internet pada Juni 2012, ada sekitar 7 miliar orang yang menggunakan internet di seluruh dunia dan pertumbuhan penduduk penggunaan internet adalah 566,4% selama periode 2000-2012 (1). Hampir semua aspek kehidupan tergantung pada teknologi komputer. Internet memiliki berbagai manfaat yang menyediakan pengguna untuk melakukan transaksi perbankan *online*, mengecek pesan elektronik, dan mencari informasi. Selain manfaat internet, ada penjahat *cyber* yang memanfaatkan alat dan mencoba untuk mendapatkan akses tidak sah ke sistem komputer untuk keuntungan mereka sendiri.

Selama komputer terhubung ke jaringan atau internet, resiko komputer terinfeksi menjadi lebih tinggi. *Hacker* dapat menggunakan serangan *malware* sebagai cara untuk menembus ke dalam jaringan dan menginfeksi komputer. Menurut Robert M (2), *malware* adalah singkatan dari *malicious software* yang dikonfigurasi dengan baik oleh penyerang untuk menyebabkan kerusakan pada jaringan komputer, *server* dan PC.

Dalam lingkungan bisnis, *malware* adalah salah satu masalah besar yang perlu dikhawatirkan. Setelah komputer bisnis terinfeksi oleh *malware*, penyerang memiliki kemampuan baik monitor atau kontrol aktivitas dari komputer bisnis, seperti, mencuri informasi, menyebarkan *spam* atau melakukan penipuan (3). Computer Economics Inc (4) melaporkan kerusakan di seluruh dunia disebabkan oleh *malware* secara total $ 13,3 milyar.

Di Indonesia kesadaran akan keamanan komputer masih sangat rendah. Sehingga pada November 2013 Indonesia menduduki posisi teratas sebagai Negara dengan *traffic malware* tertinggi dengan jumlah persentase serangan sebesar 38% (5). Pada dasarnya setiap pengguna telah memasang antivirus pada setiap komputer dan *firewall* untuk menyaring paket-paket yang tidak diinginkan. Namun, perlindungan antivirus dan *firewall* tidak memberikan perlindungan 100 % untuk mengamankan jaringan. Banyak malwares tidak terdeteksi oleh antivirus.

Menurut Mary Landesman (6), perangkat lunak antivirus menyediakan perlindungan berdasarkan *signature malware* yang tercatat dalam *database*. Antivirus tidak bisa menangkap *malware* baru yang tidak tercatat dalam basis data antivirus. Akibatnya, *malware* akan menginfeksi beberapa sistem sebelum *signature* yang baru disediakan oleh penyedia antivirus. Sebagian besar pengguna tidak mengetahui adanya *malware* dalam komputer mereka / jaringan sampai *malware* diaktifkan dan menyebabkan kerusakan pada sistem mereka.

ITS (Institut Teknologi Sepuluh Nopember) sebagai universitas yang dikenal dengan infrastruktur TI (Teknologi Informasi) yang canggih harus mempertimbangkan tentang masalah ini. Seluruh sistem harus handal dan tersedia setiap kali pengguna ingin mengaksesnya. Jika sistem tidak dapat diakses atau tidak berfungsi dengan baik, reputasi ITS mungkin terpengaruh dan beberapa orang tidak percaya lagi pada sistem jaringan ITS.

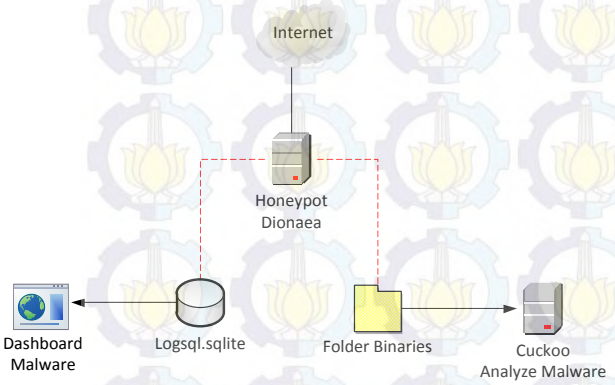
Penelitian sebelumnya yang telah dilakukan oleh Jan Goebel dan Throrsten Holz (7), untuk mendapatkan *autonomous spreading malware* dapat dilakukan dengan menggunakan bantuan *Honeypot*. Pada penelitian tersebut data *atonomous spreading malware* dikumpulkan dengan meggunakan *tools Honeypot Nepenthes*. Data *traffic* serangan *malware* yang disimpan oleh *database Nepentehes* dilakukan analisis jaringan dan *binaries malware* yang telah *terdownload* dilakukan indentifikasi jenisnya menggunakan *CWSandbox*..

Sedangkan pada penelitian ini *tools Honeypot* yang digunakan yaitu *Dionaea*. *Dionaea* merupakan versi terbaru dari *Nepenthes* yang pada tahun 2009 telah dihentikan masa pegembangannya. Identifikasi jenis *malware* pada penelitian ini menggunakan *tools Cuckoo Sanbox*. *Tools* ini dipilih karena sifatnya yang *open source* jika dibandingkan dengan

CWSanbox yang berbayar. Selain itu juga ditambahkan tools *DionaeFR* untuk memudahkan proses pembacaan informasi dari *log honeypot dionaea* agar dapat diakses secara *real time* dalam bentuk web.

II. METODOLOGI

A. *Desain Model Penelitian*



Gambar II.1 Desain Model Penelitian

Pada gambar II.1 menunjukkan desain model dari penelitian ini. Terdapat dua buah komputer yang digunakan yaitu sebagai sensor *honeypot* dan sebagai *tools* analisis *malware*. Komputer yang pertama dilakukan instalasi dan konfigurasi honeypot dionaea yang berfungsi untuk meng-*capture* dari aktifitas *malware*. Selain itu pada komputer satu juga dilakukan instalasi dan konfigurasi *DionaeFR* yang berguna untuk menampilkan informasi *log dionaea* ke dalam bentuk *dashboard*. Untuk komputer yang kedua dilakukan instalasi dan konfigurasi *cuckoo* yang berguna sebagai *tools* analisis *malware*.

Proses pengumpulan data pada peneltian ini bermula dari pemasangan honeypot dionaea di jaringan ITS-Net dengan menggunakan IP publik. Honeypot dionaea dijalankan selama 4 bulan. Dari sensor honeypot dionaea akan menghasilkan *database log* dalam format sqlite dan kumpulan *autonomous spreading malware* yang telah berhasil di-*download* ke dalam folder *binaries*. Proses berikutnya untuk mengetahui jenis *malware* perlu dilakukan indentifikasi dengan cara menyalin folder *binaries* yang ada pada komputer satu ke komputer dua. *Binaries malware* yang sudah ada pada komputer dua akan dipilih 10 dan kemudian dilakukan analisis dengan menggunakan *cuckoo*. *Report* yang dihasilkan oleh *cuckoo* akan diambil informasinya sebagai hasil dari identifikasi *malware*.

Pada tahapan terakhir dilakukan analisis yang akan ditampilkan pada bagian hasil dan pembahasan. Ada dua analisis yang dilakukan yaitu: analisis *log honeypot dionaea* dan analisis *malware* dengan *cuckoo*. Analisis *log honeypot dionaea* akan mendeskripsikan serangan *malware* berdasarkan info jaringan. Sedangkan analisis *malware* dengan cuckoo akan menghasilkan identifikasi jenis *malware*.

B. *Desain Topologi Jaringan*

Pada penelitian ini *system honeypot* diletakkan pada bagian luar *firewall*. Hal ini dipilih agar *sensor honeypot* juga dapat meng-*capture* trafik dari luar jaringan ITS-Net. Topologi jaringan yang tertera pada gambar 2 merupakan bagian kecil dari topologi jaringan ITS-Net. Untuk peletakan *honeypot dionaea* akan diletakkan di depan *gateway* agar koneksi yang ditangkap oleh *honeypot dionaea* merupakan koneksi trafik murni dari luar tanpa adanya filter dari *gateway*.

Sensor *honeypot Dionaea* dipasang pada sebuah komputer yang terhubung secara langsung dengan *router* utama yang bernama *FREY*. Sensor *Dionaea* sengaja diletakkan di luar *firewall* dan menggunakan *ip* publik agar dapat secara langsung menerima trafik dari manapun.

C. *Spesifikasi Hardware*

Pada penelitian ini menggunakan dua buah komputer yang sama dengan detai spesifikasi yaitu:

- Intel Dual Core D2500 1.86 Ghz
- OS Ubuntu 12.04.4 Desktop Edition
- 2GB RAM
- 320GB HDD

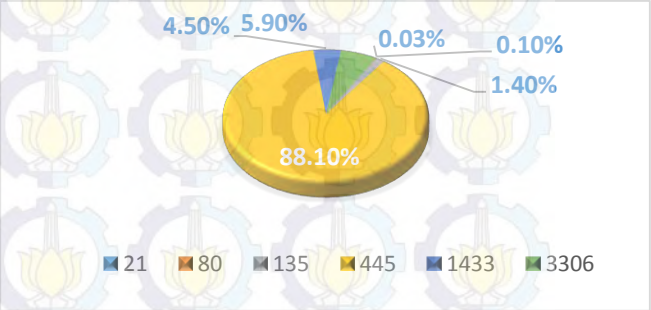
III. HASIL DAN PEMBAHASAN

A. *Analisis Log Honeypot Dionaea*

Dionaea telah dijalankan dari bulan April 2014 sampai Juli 2014. Dari hasil pengamatan selama beberapa bulan tersebut didapatkan berbagai macam data *malware*. *Dionaea* bekerja menyimpan data malware yang telah berhasil di *download* ke dalam *folder binaries*. Selain itu seluruh trafik yang telah masuk ke dalam *dionea* akan disimpan ke dalam sebuah *file log* dalam format *sqlite*.

1) *Jumlah Serangan Berdasarkan Ports*

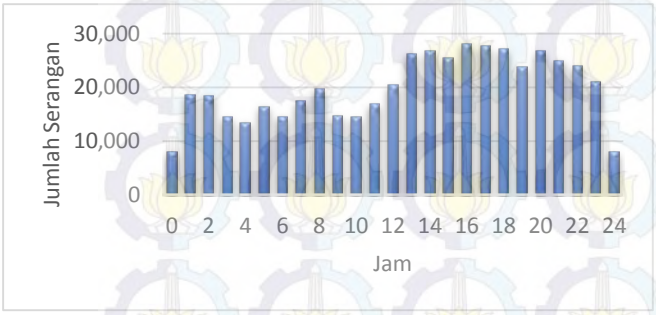
Dari hasil perekaman *honeypot Dionaea* telah didapatkan informasi *port-port* berapa saja yang sering digunakan oleh *malware* untuk melakukan penyerangan. Terdapat 6 *port* yang menjadi celah untuk masuknya malware, yaitu; 21, 80, 135, 445, 1433 dan 3306. Port 21 adalah port yang digunakan sebagai servis FTP (*File Transfer Protocol*), merupakan standar untuk pentransferan *file* antar computer.



Gambar III.1 Persentase Serangan Port oleh Malware

Port 445 menjadi *port* yang paling banyak digunakan oleh *malware* jika dibandingkan dengan *port* lain. Apabila sebuah *malware* dapat menguasai *port* ini maka akibatnya komputer *remote host* penyerang dapat mengambil atau memasukkan *file* pada komputer *host* korban dengan mudah tanpa memerlukan ijin akses.

2) Jumlah Serangan Berdasarkan Jam

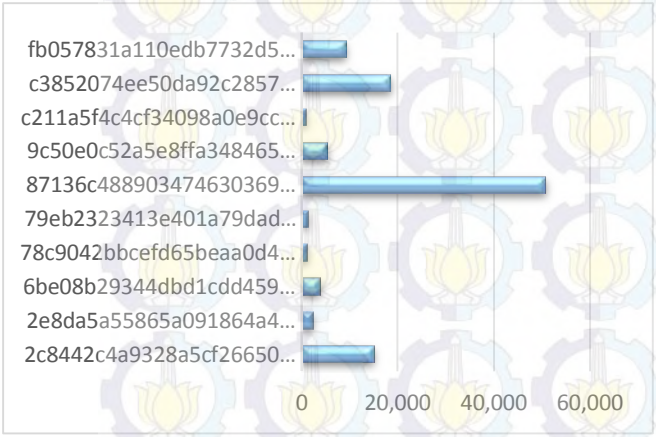


Gambar III.2 Grafik Serangan Berdasarkan Jam

Pada Gambar III.2 menampilkan grafik visualisasi terjadinya serangan *malaware* berdasarkan waktu serangan. Sepanjang waktu mulai pukul 00-24 serangan terus aktif bermunculan dengan jumlah rata-rata serangan perjam sebanyak 19.000 kali. Adanya peningkatan serangan *malware* terjadi mulai pukul 12 siang sampai pukul 4 sore, yang kemudian secara perlahan jumlah serangan mulai berkurang sedikit demi sedikit hingga akhirnya pukul 12 tengah malam jumlah serangan turun drastis.

3) 10 Malware Tertinggi

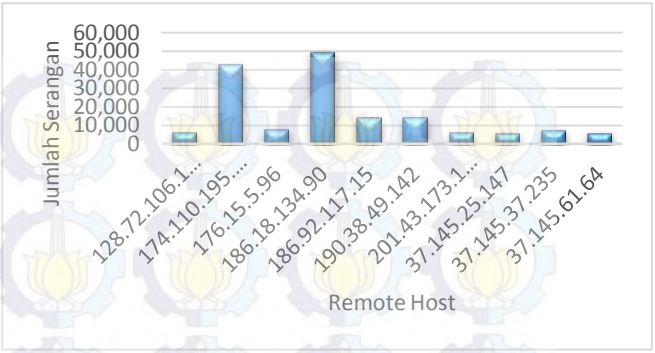
Pada Gambar III.3 menampilkan data 10 *malware* yang paling aktif menyerang *honeypot Dionaea*. Nama *malware* yang ditangkap oleh *honeypot Dionaea* menggunakan format *hash MD5* sehingga menghasilkan nama yang panjang dan acak. Dari sekian banyak *malware* yang berhasil di-*download* oleh *honeypot Dionaea*, *malware* dengan nama *87136c488903474630369e232704fa4d* menjadi *malware* yang paling aktif melakukan penyerangan dengan jumlah serangan sebanyak 50.746 kali.



Gambar III.3 Grafik 10 Malware Tertinggi

4) Jumlah Serangan Berdasarkan Remote Host

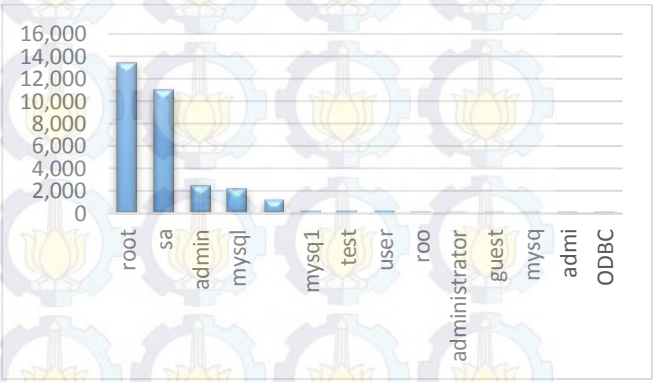
Pada Gambar III.4 menampilkan informasi 10 komputer *remote host* yang paling aktif melakukan serangan pada *honeypot Dionaea* dari total komputer *remote host* berjumlah 3151. Komputer remote host dengan alamat IP 186.18.134.90 menjadi penyerang teraktif dengan jumlah serangan 48.893 kali. Alamat IP tersebut merupakan IP yang berasal dari Negara Argentina.



Gambar III.4 Grafik Serangan Oleh Remote Host

5) Jumlah Serangan Berdasarkan Username Login

Honeypot Dionaea juga merekam akifitas *malware* yang berusaha untuk melakukan percobaan *login* ke dalam sistem. Pada Gambar III.5 dapat ditunjukkan bahwa *malware* melakukan penyerangan *login* dengan menggunakan kata kunci yang bisanya menjadi *username default*, seperti: root, sa, mysql, user, administrator, dst.



Gambar III.5 Grafik Jumlah Serangan Berdasarkan Username Login

B. Analisis Malware dengan Cuckoo

Data yang telah didapatkan dari menjalankan *honeypot Dionaea* adalah berupa *autonomous spreading malware*. Keadaan malware yang didapatkan berupa *file* dengan nama *hash MD5* dan tidak memiliki ekstensi *file*. Oleh karena itu diperlukan tahapan lebih lanjut agar bisa dilakukan identifikasi untuk mengetahui jenis *malware* apa saja yang telah berhasil didapatkan dari jaringan ITS NET. Dari pengamatan *honeypot Dionaea* yang telah berjalan didapatkan data *binaries malware* berjumlah 362. Sebanyak 10 data *malware* dipilih untuk dilakukan analisis untuk mengetahui jenis dan perilakunya. Dari 10 binaries *malware* yang berhasil diidentifikasi dapat dikelompokkan ke dalam empat kategori sebagai berikut:

1) Malware Jenis Worm

- 285d22518bbae8b1c7bba74c6c0b1a82
  Malware menginfeksi dengan cara membuat dua buah *file* dengan nama sbkpc.vbs dan WBSC.bat yang secara otomatis akan tersalin pada komputer korban. Dari hasil pengamatan *malware* akan menginfeksi program cmd.exe dan csript.exe yang merupakan program

bawaan sistem operasi windows. Dengan bantuan cmd.exe *malware* akan melakukan perubahan *registry* pada sistem, salah satu yang dilakukan yaitu merubah nama komputer. *Malware* ini juga secara diam-diam menggandakan file yang ada untuk disalin ke dalam *folder share*.

- 9a7f52b83f678f631b4e3bf092ae7ac9
  Malware ini dikategorikan sebagai *Worm* karena ketika malware ini berjalan akan membuat dua buah file baru. File pertama dengan nama sfc.exe yang berada pada folder "c:\windows\system32\". Kedua file dengan nama regedit.exe yang berada pada filder "c:\windows\".
- 57bba3322bd6bea775c1162ac1fddf3f
  Malware melakukan klamufase dalam bentuk file gambar dengan ekstensi .jpg. *Worm* ini sangat aktif di jaringan untuk berkomunikasi dengan *host* sebanyak 26 IP dan *domain* sebanyak 33 serta koneksi HTTP sebanyak 90 kali. Koneksi HTTP yang dilakukan untuk men-*dowload file-file* tertentu seperti: 0469f6cdce10e99ec75d7936ab64b3[1].css, FE69D3DCE7BF8E6244AEA97DECAD4A[1].jpg, user@adnxs[2].txt, dst.

2) Malware Jenis Botnet

- 22743a4395a36c30a5e4e8b3fa8e8543
  Pada saat *malware* dieksekusi akan membuat *file* penggandaan diri ke dalam *folder* "C:\WINDOWS\system32\" dengan nama file "qtplugin.exe". Hal ini dilakukan untuk mengelabuhi *user* sehingga mengira *malware* tersebut merupakan *file* program bawaan dari sistem operasi windows. *Malware* ini juga berusaha membuat *file* dengan nama tcp6 namun gagal dilakukan. Kemungkinan *file* tersebut akan dibuat untuk melakukan settingan IPv6 pada komputer korban. Perubahan registry pada "Software\Microsoft\Windows\CurrentVersion\Run" juga dilakukan untuk membuat *malware* ini otomatis berjalan ketika windows startup. Koneksi dengan emote host dapat dilakukan oleh malware ini dengan meggunakan alamat IP 96.9.139.213 port 1044.
- 3ab6487dff0d670645e94f240bfd2c2c
  Hasil analisis *malware* ini sama dengan *binaries malware* 22743a4395a36c30a5e4e8b3fa8e8543. Yang membedakan *malware* ini dengan yang sebelumnya yaitu cara berkomnikasi *malware* ini dengan komputer *remote host* menggunakan alamat IP 89.149.244.208.

3) Malware Jenis Trojan

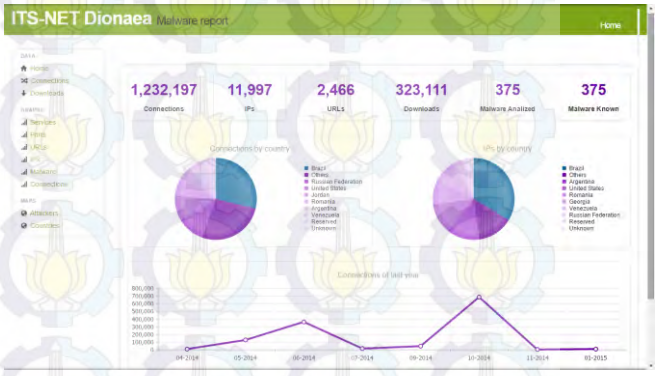
- 333def0dfdba55d936f987c7c6279f48
  Malware bekerja layaknya program *keylogger* yang akan merekam segala aktifitas *keyboard user* sehingga bisa menghasilkan data pribadi penting seperti (*username, password, pin*, dll). *Malware* juga membuat *file* baru dengan nama Avsgccs.scr yang diletakkan dalam *folder* "%CommonPrograms%\startup\". Hal tersebut membuat *trojan* dapat berjalan otomatis pada windows *startup*. *Trojan* juga terhubung dengan *domain host* gsmtp185.google.com dan teumsnj.land.ru. Jika melihat nama domain gsmtp185.google.com ada kemungkinan *malware* ini melakukan persebaran menggunakan email.
- d1d01439bf404998853790193cc0c79c
  Malware melakukan *drop file* sebanyak 6 buah yaitu, _eviip.tmp, Scrif18b5.dll, dp1.fne, del_file_b.bat, Exmlrpc.fne, krnln.fnr, ScriptBocking.dll, malware.exe dan Groove12.pip. Dengan begitu banyak file yang dibuat, malaware ini mampu menghambat kinerja sistem operasi komputer yang terinfeksi. *Malware* ini juga melakukan koneksi ke domain www.ncsoftgame.com.
- 73dc2446341699857aaf39489508f7d7
  Malware melakukan permintaan koneksi untuk terhubung dengan *host* IP 81.95.147.107, 65.55.56.206 dan 239.255.255.250. *Trojan* ini membuat dua buah *file* baru dengan nama a.bat dan 73dc2446341699857aaf39489508f7d7.exe
- 92d9980656316d0ca797e3cad1d7e684
  Malware akan membuat file baru denga nama kdalh.exe yang diletakkan ke dalam folder "C:\WINDOWS\system32\". Selain itu juga membuat file explorer.exe palsu. *Trojan* ini berusaha melakuan pembacaan data sensitif pada *history ,cookies* dan *cache* yang ada pada program *internet explorer*.

4) Malware Jenis Spyware

- 4ae984f0e9349b85f6890d67c4db3656
  Malware ini dikategorikan sebagai *spyware* yang bekerja dengan mengumpulkan informasi pribadi dengan cara merubah *registry*, *cookies*, *history* dan *cache*. Informasi pribadi yang telah berhasil dicuri oleh *malware* akan dikirimkan ke *remote host* dengan IP 81.19.78.85. IP tersebut merupakan IP dari *domain* mail.rambler.ru. Ternyata pembuat *malware* memanfaatkan email sebagai media penampungan data informasi dari hasil pencurian.

C. Dashboard Statistic Malware

Untuk memudahkan pembacaan *log dionaea* dan agar dapat dilakukan monitoring secara *real time* maka ditambahkan *tools DionaeFR*. *Tools* ini berfungsi untuk membaca *file log* dari dionaea yang berformat *database sqlite* dan menampilkannya dalam bentuk web.



Gambar III.6 Halaman Utama Dashboard

Halaman utama pada dashboard menampilkan informasi ringkas mengenai *statistic malware* mulai dari; *connection, IP, URL, download, chart* persetase *connection by country*, *chart* persentase *IP by country* dan grafik *connection by month*. Untuk dapat melihat informasi yang lebih detail dapat menggunakan menu *graph* yang terdiri dari iformasi; *services, ports, URL, IP, malware* dan *connection*. Selain itu juga terdapat visualisasi data dalam bentuk map untuk

menampilkan informasi *attacker* (penyerang) dan *countries* (penyerang berdasarkan Negara).

IV. KESIMPULAN

A. *Kesimpulan*

Dari pelaksanaan penelitian tugas akhir ini di dapatkan kesimpulan :

1. Selama monitoring *honeypot Dionaea* dijalankan pada bulan April 2014 sampai Juli 2014 telah didapatkan serangan mawalre sebanyak 322537 kali.
2. *Unique binaries malware* yang berhasil di-*download honeypot Dionaea* sebanyak 362 *file*.
3. Persentase *port* yang sering diserang oleh *malware* yaitu port 445 sebesar 88%, karena dengan *port* ini *malware* dapat melakukan pencurian file yang ada pada komputer. Sedangkan *port* 3306 sebesar 6%, melaui *port* ini penyerang berusaha mencari celah kemanan pada *database mysql*.
4. Berdasarkan waktu serangan *malware*, aktifitas serangan *malware* tertinggi terjadi pada sore hari pukul 16.00-17.00.
5. Dari hasil identifikasi *autonomous spreading malware* dengan menggunakan *Cuckoo* diapatkan bahwa presentase *malware* yang ditemukan yaitu jenis *Trojan sebanyak 40%, Worm sebanyak 30%, Botnet* sebanyak 20% dan *Spyware* sebanyak 10%.
6. Dari jumlah trafik yang masuk sebanyak 482.426 kali, persentase trafik yang diterima sebesar 67% dan yang ditolak 33% .

B. *Saran*

Dari pelaksanaan penelitian tugas akhir ini dapat diberikan saran untuk penelitian selanjutnya antara lain :

1. Menggunakan *tools honeypot* lain yang berjenis *high interaction honeypot* untuk menghasilkan informasi yang lebih detail.
2. Menggunakan beberapa *tools honeypot* yang berbeda dalam satu waktu sehingga dapat dilihat perbandingan antara *tools* yang satu dengan yang lain.

V. DAFTAR PUSTAKA

1. Miniwatts Marketing Group. World Internet Users Statistics Usage and World Population Stats. [Online] 30 Juni 2012. [Dikutip: 26 Februari 2014.] http://www.internetworldstats.com/stats.htm.

2. Moir, Robert. Microsoft TechNet. [Online] Oktober 2003. [Dikutip: 26 Februari 2014.] http://technet.microsoft.com/en-us/library/dd632948.aspx.

3. Internet Identity. [Online] 2011. [Dikutip: 26 Februari 2014.] http://www.internetidentity.com/problems/phishing-and-malware.

4. Computer Economics. [Online] Juni 2007. [Dikutip: 26 Februari 2014.] http://www.computereconomics.com/article.cfm?id=1225.

5. Giri, Ignatius. Blog ESET Indonesia. [Online] 1 November 2013. [Dikutip: 26 Februari 2014.] http://blog.eset.co.id/index.php/traffic-serangan-malware-indonesia-nomor-satu-di-dunia-ini-penyebabnya/.

6. Landesman, Mary. About.com Antivirus Software. [Online] [Dikutip: 26 Februari 2014.] http://antivirus.about.com/od/antivirusglossary/a/What-Is-Antivirus-Software.htm.

7. *Measurement and Analysis of Autonomous Spreading Malware in a University Environment.* Gobel, Jan, Holz, Thorsten dan Willems, Carsten. 2007.

8. Splitzner, Lance. *Honeypots: Tracking Hackers.* s.l. : Addison Wesley, 2002.

9. IT, Carnivore. dionaea — catches bugs. [Online] http://dionaea.carnivore.it/.

10. Cuckoo Sandbox Book — Cuckoo Sandbox v1.1 Book. [Online] Cuckoo Foundation, 2014. http://docs.cuckoosandbox.org/en/latest/.